

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-084271

(43)Date of publication of application : 22.03.2002

(51)Int.Cl.

H04L 9/08

G11B 20/10

(21)Application number : 2000-270919

(71)Applicant : SONY CORP

(22)Date of filing : 07.09.2000

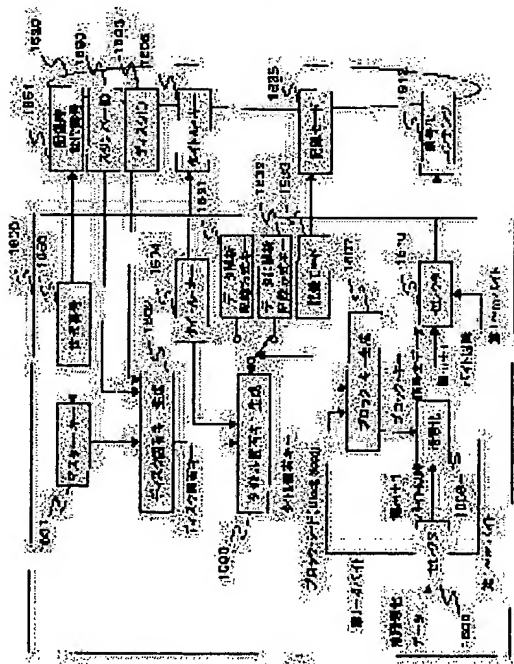
(72)Inventor : ASANO TOMOYUKI
OSAWA YOSHITOMO

(54) INFORMATION RECORDING APPARATUS, INFORMATION REPRODUCING DEVICE, INFORMATION RECORDING METHOD, INFORMATION REPRODUCING METHOD, AND INFORMATION RECORDING MEDIUM, AND PROGRAM PROVIDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an information recording apparatus and reproducing devices that can effectively exclude utilization of illegal contents.

SOLUTION: The recording medium of this invention stores secret information whose write/read method is difficult for its analysis and that can be read only by a special read method, and the secret information is used for an encryption key for encryption or decoding processing of contents in recording or reproducing contents such as music data image data to/from the recording medium. The secret information is e.g. a stamper ID, and the stamper ID as the secret information, a master key and a medium key or the like distributed through key distribution configuration of a tree structure are used to generate an encryption processing key for contents. Thus, a special read method as to the secret information can be performed and only a legal device to which the key is distributed through the key distribution configuration of a tree structure can utilize contents.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-84271

(P2002-84271A)

(43)公開日 平成14年3月22日(2002.3.22)

(51) Int.Cl.⁷

識別記号

FI

テーマコード(参考)

H04L 9/08

G 1 1 B 20/10

H 5 D 0 4 4

G 1 1 B 20/10

H04L 9/00

601D 5J104

審査請求 未請求 請求項の数40 OL (全 56 頁)

(21)出願番号 特願2000-270919(P2000-270919)

(22)出願日 平成12年9月7日(2000.9.7)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 浅野 智之

東京都品川区北品川6丁目7番35号 ソニ
一株式会社内

(72)発明者 大澤 義知

東京都品川区北品川6丁目7番35号 ソニ
一株式会社内

(74)代理人 100101801

弁理士 山田 英治 (外2名)

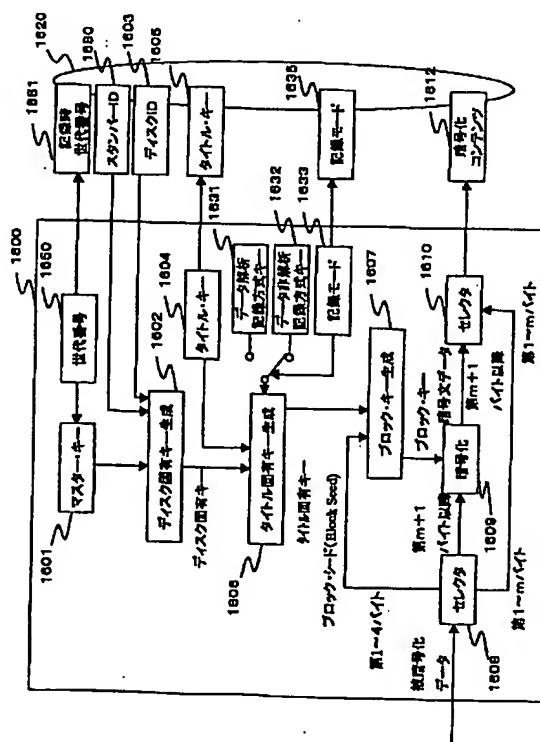
最終頁に続く

(54)【発明の名称】 情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体

(57) 【要約】

【課題】 不正なコンテンツの利用を効果的に排除可能とした情報記録、再生装置を提供する。

【解決手段】 記録媒体に、あらかじめその書き込み／読み出し方法が解析困難な、特殊の読み出し方法でのみ読み取り可能な秘密情報を格納し、記録媒体に対する音楽データ、画像データ等のコンテンツの記録あるいは再生を行う際のコンテンツ暗号化あるいは復号処理用暗号鍵に、上記秘密情報を作用させる。秘密情報は、例えばスタンパーIDであり、秘密情報としてのスタンパーIDと、ツリー構造の鍵配布構成により配布されるマスターキー、メディアキー等と共にコンテンツの暗号処理鍵の生成を行なう。従って、秘密情報についての特殊な読み取り方法を実行可能で、かつツリー構造の鍵配布構成により鍵の配布された正当デバイスでのみコンテンツの利用が可能となる。



【特許請求の範囲】

【請求項 1】記録媒体に情報を記録する情報記録装置において、

記録媒体に対する格納データの暗号化処理を実行する暗号処理手段と、

記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理手段と、を有し、

前記暗号処理手段は、

前記秘密情報復号処理手段において記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号化処理を実行する構成を有することを特徴とする情報記録装置。

【請求項 2】前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパー ID、または個々の記録媒体に固有なディスク ID、コンテンツ毎に異なって設定するコンテンツ ID、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理手段は、記録媒体から読み取られた秘密情報の復号処理を実行する構成を有することを特徴とする請求項 1 に記載の情報記録装置。

【請求項 3】前記暗号処理手段は、

前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ暗号化キーを生成する構成であり、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行わず、前記暗号処理部内で実行されるコンテンツ暗号化キー生成処理においてのみ利用可能な構成としたことを特徴とする請求項 1 に記載の情報記録装置。

【請求項 4】前記情報記録装置は、さらに、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、

前記暗号処理手段は、

前記秘密情報復号処理手段において読み取られた秘密情報と、前記情報記録装置に内蔵した暗号化キー生成用データに基づいて前記コンテンツ暗号化キーを生成する構成であり、

前記暗号化キー生成用データは、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック (EKB) によって更新可能なデータとして構成されていることを特徴とする請求項 1 に記載の情報記録装置。

【請求項 5】前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする請求項 4 に記載の情報記録装置。

【請求項 6】前記暗号化キー生成用データは、更新情報

としての世代番号が対応付けられた構成であり、

前記暗号処理部は、

前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする請求項 4 に記載の情報記録装置。

【請求項 7】前記情報記録装置は、さらに、

トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報 (ATS) を付加するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、

前記受信時刻情報 (ATS) の付加された 1 以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、

前記記録媒体に対する格納データの暗号化処理においては、前記秘密情報と、前記暗号化キー生成用データと前記受信時刻情報 (ATS) を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成する構成を有することを特徴とする請求項 4 に記載の情報記録装置。

【請求項 8】前記秘密情報復号処理手段は、

秘密情報を形成するビット列を 2 進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する構成を有し、

前記 2 進数系列を生成し、生成 2 進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行する構成を有することを特徴とする請求項 1 に記載の情報記録装置。

【請求項 9】前記秘密情報復号処理手段は、

秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行する構成を有することを特徴とする請求項 1 に記載の情報記録装置。

【請求項 10】記録媒体に記録された情報を再生する情報再生装置において、

記録媒体から読み取られるデータの復号処理を実行する暗号処理手段と、

記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理手段と、を有し、

前記暗号処理手段は、

前記秘密情報復号処理手段において記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する構成を有することを特徴とする情報再生装置。

【請求項 11】前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタ

ンパーID、または個々の記録媒体に固有なディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理手段は、記録媒体から読み取られた秘密情報の復号処理を実行する構成を有することを特徴とする請求項10に記載の情報再生装置。

【請求項12】前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ復号キーを生成する構成であり、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行わず、前記暗号処理部内で実行されるコンテンツ復号キー生成処理においてのみ利用可能とした構成を有することを特徴とする請求項10に記載の情報再生装置。

【請求項13】前記情報再生装置は、さらに、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報と、前記情報再生装置に内蔵した復号キー生成用データに基づいて前記コンテンツ復号キーを生成する構成であり、前記復号キー生成用データは、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック(EKB)によって更新可能なデータとして構成されていることを特徴とする請求項10に記載の情報再生装置。

【請求項14】前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする請求項13に記載の情報再生装置。

【請求項15】前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体からのデータ再生時に、使用した前記復号キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする請求項13に記載の情報再生装置。

【請求項16】前記情報再生装置は、さらに、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報(ATS)を付加するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、前記受信時刻情報(ATS)の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、前記記録媒体からのデータの復号処理においては、前記秘密情報と、前記復号キー生成用データと前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報で

あるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成する構成を有することを特徴とする請求項13に記載の情報再生装置。

【請求項17】前記秘密情報復号処理手段は、秘密情報を形成するビット列を2進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する構成を有し、

前記2進数系列を生成し、生成2進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行する構成を有することを特徴とする請求項10に記載の情報再生装置。

【請求項18】前記秘密情報復号処理手段は、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行する構成を有することを特徴とする請求項10に記載の情報再生装置。

【請求項19】記録媒体に情報を記録する情報記録方法において、

記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、

前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、

を有することを特徴とする情報記録方法。

【請求項20】前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーID、または個々の記録媒体に固有なディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理ステップは、記録媒体から読み取られた秘密情報の復号処理を実行することを特徴とする請求項19に記載の情報記録方法。

【請求項21】前記暗号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ暗号化キーを生成するステップを含み、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行わず、前記暗号処理部内で実行されるコンテンツ暗号化キー生成処理においてのみ利用可能としたことを特徴とする請求項19に記載の情報記録方法。

【請求項22】前記情報記録方法において、前記暗号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報と、情報記録装置に内蔵した暗号化キー生成用データに基づいて前記コンテンツ暗号化キーを生成するステッ

ブを含み、

前記暗号化キー生成用データは、複数の異なる情報記録装置をリーフとし、各分岐をノードとして各ノード、リーフに固有のキーを設定した階層ツリー構造のノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キープロック(EKB)によって更新可能なデータであることを特徴とする請求項19に記載の情報記録方法。

【請求項23】前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする請求項22に記載の情報記録方法。

【請求項24】前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理ステップは、

前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする請求項22に記載の情報記録方法。

【請求項25】前記情報記録方法は、さらに、
トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報(ATS)を付加するトランスポート・ストリーム処理ステップを有し、

前記暗号処理ステップは、

前記受信時刻情報(ATS)の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成するステップを含み、

前記記録媒体に対する格納データの暗号処理においては、前記秘密情報と、前記暗号化キー生成用データと前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成することを特徴とする請求項22に記載の情報記録方法。

【請求項26】前記秘密情報復号処理ステップは、秘密情報を形成するビット列を2進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する復号処理ステップを含み、

該復号処理ステップは、

前記2進数系列を生成し、生成2進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行することを特徴とする請求項19に記載の情報記録方法。

【請求項27】前記秘密情報復号処理ステップは、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行することを特徴とする請求項19に記載の情報記録方法。

【請求項28】記録媒体から情報を再生する情報再生方

法において、

記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、

前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する復号処理ステップと、

を有することを特徴とする情報再生方法。

【請求項29】前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーID、または個々の記録媒体に固有なディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理ステップは、記録媒体から読み取られた秘密情報の復号処理を実行することを特徴とする請求項28に記載の情報再生方法。

【請求項30】前記復号処理ステップは、

前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ復号キーを生成するステップを含み、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行わず、前記暗号処理部内で実行されるコンテンツ復号キー生成処理においてのみ利用可能としたことを特徴とする請求項28に記載の情報再生方法。

【請求項31】前記情報再生方法において、

前記復号処理ステップは、

前記秘密情報復号処理手段において読み取られた秘密情報と、情報再生装置に内蔵した復号キー生成用データに基づいて前記コンテンツ復号キーを生成するステップを含み、

前記復号キー生成用データは、複数の異なる情報再生装置をリーフとし、各分岐をノードとして各ノード、リーフに固有のキーを設定した階層ツリー構造のノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キープロック(EKB)によって更新可能なデータであることを特徴とする請求項28に記載の情報再生方法。

【請求項32】前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする請求項31に記載の情報再生方法。

【請求項33】前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、

前記復号処理ステップは、

前記記録媒体からのデータ再生時に、使用した前記復号キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする

請求項31に記載の情報再生方法。

【請求項34】前記情報再生方法は、さらに、
 TRANSPORTパケットから成るTRANSPORTストリームを構成する各パケットに受信時刻情報(ATS)を付加するTRANSPORT・ストリーム処理ステップを有し、

前記復号処理ステップは、

前記受信時刻情報(ATS)の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成するステップを含み、
 前記記録媒体からのデータの再生処理においては、前記秘密情報と、前記復号キー生成用データと前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成することを特徴とする請求項31に記載の情報再生方法。

【請求項35】前記秘密情報復号処理ステップは、
 秘密情報を形成するビット列を2進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する復号処理ステップを含み、
 該復号処理ステップは、
 前記2進数系列を生成し、生成2進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行することを特徴とする請求項28に記載の情報再生方法。

【請求項36】前記秘密情報復号処理ステップは、
 秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行することを特徴とする請求項28に記載の情報再生方法。

【請求項37】情報を記録可能な情報記録媒体であって、
 通常格納データの読み取り態様と異なる特殊なデータ読み取り処理を実行することによってのみ再生可能な秘密情報と、
 該秘密情報を適用して生成可能な暗号処理鍵により復号可能な暗号化コンテンツを格納したことを特徴とする情報記録媒体。

【請求項38】前記秘密情報は、複数の記録媒体において共通なスタンパーID、または個々の記録媒体に固有なディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキーのいずれかのデータを含むことを特徴とする請求項37に記載の情報記録媒体。

【請求項39】記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

記録媒体に格納されたコンテンツデータの読み取り態様

と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、

前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、

を有することを特徴とするプログラム提供媒体。

10 【請求項40】記録媒体に格納された情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、
 記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、

前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する復号処理ステップと、

を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体に関し、特に、木構造の階層的鍵配信方式を用いることにより、メッセージ量を小さく抑さえ、マスターキーあるいはメディアキー等の鍵更新におけるデータ配信の負荷を軽減することを可能とした構成を提供するとともに、コンテンツの暗号処理用鍵の生成データとしてコンテンツの再生処理とは異なる特殊なデータ読み取り処理においてのみ読み取り可能な秘密情報を適用する構成により、コンテンツのセキュリティを高めることを可能とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体に関する。

【0002】具体的には、各記録再生機器をn分木の各葉(リーフ)に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵(マスターキーもしくはメディアキー)を配信し、これを用いて各装置がコンテンツデータの記録、再生を行うとともに、コンテンツ記録、再生用のコンテンツ格納ディスクにスタンパーID等を秘密情報として格納し、特定の再生処理によって秘密情報を取得して取得秘密情報に基づいてコンテンツの暗号処理用の鍵を生成する構成とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム

提供媒体に関する。

【0003】

【従来の技術】ディジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、ディジタル的に記録する記録装置や記録媒体が普及しつつある。このようなディジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにディジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなディジタルデータの不正なコピーを防ぐため、ディジタル記録装置および記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

【0004】例えば、MD（ミニディスク）（MDは商標）装置において、違法なコピーを防止する方法として、SCMS（Serial Copy Management System）が採用されている。SCMSは、データ再生側において、オーディオデータとともにSCMS信号をディジタルインタフェース（DIF）から出力し、データ記録側において、再生側からのSCMS信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

【0005】具体的にはSCMS信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、1度だけコピーが許されている（copy once allowed）データであるか、またはコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、DIFからオーディオデータを受信すると、そのオーディオデータとともに送信されるSCMS信号を検出する。そして、SCMS信号が、コピーフリー（copy free）となっている場合には、オーディオデータをSCMS信号とともにミニディスクに記録する。また、SCMS信号が、コピーを1度のみ許可（copy once allowed）となっている場合には、SCMS信号をコピー禁止（copy prohibited）に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、SCMS信号が、コピー禁止（copy prohibited）となっている場合には、オーディオデータの記録を行わない。このようなSCMSを使用した制御を行なうことで、ミニディスク装置では、SCMSによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

【0006】しかしながら、SCMSは上述のようにSCMS信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、SCMSの制御を実行す

る構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、DVDプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

【0007】コンテンツ・スクランブルシステムでは、DVD-ROM（Read Only Memory）に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー（復号鍵）が、ライセンスを受けたDVDプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、DVD-ROMに記録された暗号化データを復号することにより、DVD-ROMから画像や音声を再生することができる。

【0008】一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するためのキーを有していないため、DVD-ROMに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは、ディジタルデータを記録したDVD-ROMの再生を行なえないことになり、不正コピーが防止されるようになっている。

【0009】しかしながら、DVD-ROMで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ROMメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、RAMメディアという）への適用については考慮されていない。

【0010】即ち、ROMメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、RAMメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

【0011】そこで、本出願人は、先の特許出願、特開平11-224461号公報（特願平10-25310号）において、個々の記録媒体を識別する為の情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

【0012】この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができな

いようになっている。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

【0013】ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライ

【0014】

【発明が解決しようとする課題】ところで、上記の構成においては、ライセンスを受けた装置において格納されるマスターキーは全機器において共通であるのが一般的である。このように複数の機器に対して共通のマスターキーを格納するのは、1つの機器で記録された媒体を他の機器で再生可能とする（インターオペラビリティを確保する）ために必要な条件であるからである。

【0015】しかし、この方式においては、攻撃者が1つの機器の攻撃に成功し、マスターキーを取出した場合、全システムにおいて暗号化されて記録されているデータを復号することができてしまい、システム全体が崩壊する。これを防ぐためには、ある機器が攻撃されてマスターキーが露呈したことが発覚した場合、マスターキーを新たなものに更新し、攻撃に屈した機器以外の全機器に新たに更新されたマスターキーを与えることが必要になる。この構成を実現する一番単純な方式としては、個々の機器に固有の鍵（デバイスキー）を与えておき、新たなマスターキーを個々のデバイスキーで暗号化した値を用意し、記録媒体を介して機器に伝送する方式が考えられるが、機器の台数に比例して伝送すべき全メッセージ量が増加するという問題がある。

【0016】上記問題を解決する構成として、本出願人は、各情報記録再生装置を n 分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行うようにすることにより、正当な（秘密が露呈していない装置に）対して少ないメッセージ量でマスターキーもしくはメディアキーを伝送できる構成を、先に提案し、すでに特許出願している。具体的には、記録媒体への記録もしくは記録媒体からの再生に必要な鍵を生成するために必要となるキー、例えば n 分木の各葉（リーフ）を構成するノードに割り当てたノードキーを更新ノードキーとして設定し、更新ノードキーを正当な機器のみが有するリーフキー、

ノードキーで復号可能な態様で暗号化处理した情報を含む有効化キープロック（EKB）を各情報記録再生装置に配信し、有効化キープロック（EKB）を受信した各情報記録再生装置のEKB復号処理により、各装置が記録もしくは記録媒体からの再生に必要な鍵を取得可能とした構成である。

【0017】上述の構成は、情報記録再生装置に与えられた暗号鍵や、記録媒体へのデータの記録／再生時の暗号化／復号処理に用いるメディアキーが露呈しないことにその安全性の根拠が置かれている。従って、メディアキーの露呈が防止可能であれば問題はない。しかし、秘密とされるべきメディアキーが露呈すると、少なからずシステムに影響があるものとなっている。

【0018】本発明は、上記の問題点を解決することを目的とするものであり、通常データの読み取り手法においては、データの解析が困難な構成で書き込んだ秘密情報を記録媒体へのデータの記録／再生時の暗号化／復号処理に用いる鍵生成用のデータとして用いる構成とすることにより、コンテンツの不正利用を排除可能とするとともに、記録／再生時の暗号化／復号処理に用いる鍵用の種データの漏洩の可能性を激減させたセキュリティの高い情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

【0019】

【課題を解決するための手段】本発明の第1の側面は、記録媒体に情報を記録する情報記録装置において、記録媒体に対する格納データの暗号化处理を実行する暗号処理手段と、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理手段と、を有し、前記暗号処理手段は、前記秘密情報復号処理手段において記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号化处理を実行する構成を有することを特徴とする情報記録装置にある。

【0020】さらに、本発明の情報記録装置の一実施態様において、前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーID、または個々の記録媒体に固有なディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理手段は、記録媒体から読み取られた秘密情報の復号処理を実行する構成を有することを特徴とする。

【0021】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ暗号化キーを生成する構成であり、読み取られた秘

密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行わず、前記暗号処理部内で実行されるコンテンツ暗号化キー生成処理においてのみ利用可能な構成としたことを特徴とする。

【0022】さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、さらに、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報と、前記情報記録装置に内蔵した暗号化キー生成用データに基づいて前記コンテンツ暗号化キーを生成する構成であり、前記暗号化キー生成用データは、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック (EKB) によって更新可能なデータとして構成されていることを特徴とする。

【0023】さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする。

【0024】さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする。

【0025】さらに、本発明の情報記録装置の一実施態様において、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報 (ATS) を付加するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、前記受信時刻情報 (ATS) の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、前記記録媒体に対する格納データの暗号処理においては、前記秘密情報と、前記暗号化キー生成用データと前記受信時刻情報 (ATS) を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成する構成を有することを特徴とする。

【0026】さらに、本発明の情報記録装置の一実施態様において、前記秘密情報復号処理手段は、秘密情報を形成するビット列を2進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する構成を有し、前記2進数系列を生成し、生成2進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行する構成を有することを特徴とする。

【0027】さらに、本発明の情報記録装置の一実施態

様において、前記秘密情報復号処理手段は、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行する構成を有することを特徴とする。

【0028】さらに、本発明の第2の側面は、記録媒体に記録された情報を再生する情報再生装置において、記録媒体から読み取られるデータの復号処理を実行する暗号処理手段と、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理手段と、を有し、前記暗号処理手段は、前記秘密情報復号処理手段において記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する構成を有することを特徴とする情報再生装置にある。

【0029】さらに、本発明の情報再生装置の一実施態様において、前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーID、または個々の記録媒体に固有なディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理手段は、記録媒体から読み取られた秘密情報の復号処理を実行する構成を有することを特徴とする。

【0030】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ復号キーを生成する構成であり、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行わず、前記暗号処理部内で実行されるコンテンツ復号キー生成処理においてのみ利用可能な構成を有することを特徴とする。

【0031】さらに、本発明の情報再生装置の一実施態様において、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報と、前記情報再生装置に内蔵した復号キー生成用データに基づいて前記コンテンツ復号キーを生成する構成であり、前記復号キー生成用データは、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック (EKB) によって更新可能なデータとして構成されていることを特徴とする。

【0032】さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特

徴とする。

【0033】さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体からのデータ再生時に、使用した前記復号キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする。

【0034】さらに、本発明の情報再生装置の一実施態様において、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報 (ATS) を付加するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、前記受信時刻情報 (ATS) の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、前記記録媒体からのデータの復号処理においては、前記秘密情報と、前記復号キー生成用データと前記受信時刻情報 (ATS) を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成する構成を有することを特徴とする。

【0035】さらに、本発明の情報再生装置の一実施態様において、前記秘密情報復号処理手段は、秘密情報を形成するビット列を2進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する構成を有し、前記2進数系列を生成し、生成2進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行する構成を有することを特徴とする。

【0036】さらに、本発明の情報再生装置の一実施態様において、前記秘密情報復号処理手段は、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行する構成を有することを特徴とする。

【0037】さらに、本発明の第3の側面は、記録媒体に情報を記録する情報記録方法において、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、を有することを特徴とする情報記録方法にある。

【0038】さらに、本発明の情報記録方法の一実施態様において、前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーID、または個々の記録媒体に固有なディスクID、コンテンツ毎に異なって設定するコンテンツID、

あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理ステップは、記録媒体から読み取られた秘密情報の復号処理を実行することを特徴とする。

【0039】さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ暗号化キーを生成するステップを含み、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行わず、前記暗号処理部内で実行されるコンテンツ暗号化キー生成処理においてのみ利用可能としたことを特徴とする。

【0040】さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報と、情報記録装置に内蔵した暗号化キー生成用データに基づいて前記コンテンツ暗号化キーを生成するステップを含み、前記暗号化キー生成用データは、複数の異なる情報記録装置をリーフとし、各分岐をノードとして各ノード、リーフに固有のキーを設定した階層ツリー構造のノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック (EKB) によって更新可能なデータであることを特徴とする。

【0041】さらに、本発明の情報記録方法の一実施態様において、前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする。

【0042】さらに、本発明の情報記録方法の一実施態様において、前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理ステップは、前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする。

【0043】さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報 (ATS) を付加するトランスポート・ストリーム処理ステップを有し、前記暗号処理ステップは、前記受信時刻情報 (ATS) の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成するステップを含み、前記記録媒体に対する格納データの暗号処理においては、前記秘密情報と、前記暗号化キー生成用データと前記受信時刻情報 (ATS) を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成することを特徴とする。

【0044】さらに、本発明の情報記録方法の一実施態様において、前記秘密情報復号処理ステップは、秘密情報を形成するビット列を2進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する復号処理ステップを含み、該復号処理ステップは、前記2進数系列を生成し、生成2進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行することを特徴とする。

【0045】さらに、本発明の情報記録方法の一実施態様において、前記秘密情報復号処理ステップは、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行することを特徴とする。

【0046】さらに、本発明の第4の側面は、記録媒体から情報を再生する情報再生方法において、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する復号処理ステップと、を有することを特徴とする情報再生方法にある。

【0047】さらに、本発明の情報再生方法の一実施態様において、前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーID、または個々の記録媒体に固有なディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理ステップは、記録媒体から読み取られた秘密情報の復号処理を実行することを特徴とする。

【0048】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ復号キーを生成するステップを含み、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行わず、前記暗号処理部内で実行されるコンテンツ復号キー生成処理においてのみ利用可能としたことを特徴とする。

【0049】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報と、情報再生装置に内蔵した復号キー生成用データに基づいて前記コンテンツ復号キーを生成するステップを含み、前記復号キー生成用データは、複数の異なる情報再生装置をリーフとし、各分岐をノードとして各ノード、リーフに固有のキーを設定した階層ツリー構造のノードキーを下位階

層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キープロック(EKB)によって更新可能なデータであることを特徴とする。

【0050】さらに、本発明の情報再生方法の一実施態様において、前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする。

10 【0051】さらに、本発明の情報再生方法の一実施態様において、前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記復号処理ステップは、前記記録媒体からのデータ再生時に、使用した前記復号キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする。

【0052】さらに、本発明の情報再生方法の一実施態様において、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報(ATS)を付加するトランスポート・ストリーム処理20 ステップを有し、前記復号処理ステップは、前記受信時刻情報(ATS)の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成するステップを含み、前記記録媒体からのデータの再生処理においては、前記秘密情報と、前記復号キー生成用データと前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成することを特徴とする。

30 【0053】さらに、本発明の情報再生方法の一実施態様において、前記秘密情報復号処理ステップは、秘密情報を形成するビット列を2進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する復号処理ステップを含み、該復号処理ステップは、前記2進数系列を生成し、生成2進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行することを特徴とする。

【0054】さらに、本発明の情報再生方法の一実施態様において、前記秘密情報復号処理ステップは、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行することを特徴とする。

【0055】さらに、本発明の第5の側面は、情報を記録可能な情報記録媒体であって、通常格納データの読み取り態様と異なる特殊なデータ読み取り処理を実行することによってのみ再生可能な秘密情報と、該秘密情報を適用して生成可能な暗号処理鍵により復号可能な暗号化コンテンツを格納したことを特徴とする情報記録媒体に40 ある。

【0056】さらに、本発明の情報記録媒体の一実施態様において、前記秘密情報は、複数の記録媒体において共通なスタンパーID、または個々の記録媒体に固有なディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキーのいずれかのデータを含むことを特徴とする。

【0057】さらに、本発明の第6の側面は、記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、を有することを特徴とするプログラム提供媒体にある。

【0058】さらに、本発明の第7の側面は、記録媒体に格納された情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する復号処理ステップと、を有することを特徴とするプログラム提供媒体にある。

【0059】

【作用】本発明の構成においては、記録媒体に、あらかじめその書き込み/読出し方法の解析の困難な秘密情報からなる信号を埋め込んでおく。この記録媒体に対してデータの記録/再生を行う際のデータの暗号化/復号処理を行うための暗号鍵には、上記の秘密情報を作用させる。秘密情報の読出し方法および読み出された秘密の値は記録再生装置内でたとえばLSI内に実装されて高度に保護され、露呈しない構成である。このような構成であるため、たとえ他の暗号鍵が露呈したとしても、記録媒体上に秘密情報として格納されたデータは安全に保護できる。また、記録媒体上の音楽等の各種コンテンツデータの暗号化/復号処理を行うための暗号鍵は、秘密情報を用いて生成されることになるため、コンテンツ自体の不正な復号等の処理が困難になり、セキュリティレベルの高いコンテンツ保護が可能になる。

【0060】なお、本発明の第6および第7の側面に係

るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0061】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【0062】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0063】

【発明の実施の形態】〔システム構成〕図1は、本発明を適用した記録再生装置100の一実施例構成を示すブロック図である。記録再生装置100は、入出力I/F (Interface) 120、MPEG (Moving Picture Experts Group) コーデック130、A/D、D/Aコンバータ141を備えた入出力I/F (Interface) 140、暗号処理手段150、ROM (Read Only Memory) 160、CPU (Central Processing Unit) 170、メモリ180、記録媒体195のドライブ190、さらにトランスポート・ストリーム処理手段 (TS処理手段) 300、秘密情報復号処理手段500を有し、これらはバス110によって相互に接続されている。

【0064】入出力I/F 120は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス110上に出力するとともに、バス110上のデジタル信号を受信し、外部に出力する。MPEGコーデック130は、バス110を介して供給されるMPEG符号化されたデータを、MPEGデコードし、入出力I/F 140に出力するとともに、入出力I/F 140から供給されるデジタル信号をMPEGエンコードしてバス110上に出力する。入出力I/F 140は、A/D、D/Aコンバータ141を内蔵している。入出力I/F 140は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A/D、D/Aコンバータ141でA/D (Analog Digital) 変換することで、デジタル信号として、MPEGコーデック130に出力するとともに、MPEGコーデック130からのデジタル信号を、A/D、D/Aコンバータ141でD/A (Digital Analog) 変換することで、アナログ信号として、外部に出力する。

【0065】暗号処理手段150は、例えば、1チップ

のLSI (Large Scale IntegratedCircuit)で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【0066】ROM160は、例えば、記録再生装置ごとに固有の、あるいは複数の記録再生装置のグループごとに固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。CPU170は、メモリ180に記憶されたプログラムを実行することで、MPEGコーデック130や暗号処理手段150等を制御する。メモリ180は、例えば、不揮発性メモリで、CPU170が実行するプログラムや、CPU170の動作上必要なデータを記憶する。ドライブ190は、デジタルデータを記録再生可能な記録媒体195を駆動することにより、記録媒体195からデジタルデータを読み出し(再生し)、バス110上に出力するとともに、バス110を介して供給されるデジタルデータを、記録媒体195に供給して記録させる。また、プログラムをROM160に、デバイスキーをメモリ180に記憶するようにしてもよい。

【0067】記録媒体195は、例えば、DVD、CD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ190に対して着脱可能な構成であるとする。但し、記録媒体195は、記録再生装置100に内蔵する構成としてもよい。

【0068】トランスポート・ストリーム処理手段(TS処理手段)300は、後段において図6以下を用いて詳細に説明するが、例えば複数のTVプログラム(コンテンツ)が多重化されたトランスポートストリームから特定のプログラム(コンテンツ)に対応するトランスポート packetsを取り出して、取り出したトランスポートストリームの出現タイミング情報を各packetとともに記録媒体195に格納するためのデータ処理および、記録媒体195からの再生処理時の出現タイミング制御処理を行なう。

【0069】トランスポートストリームには、各トランスポート packetsの出現タイミング情報としてのATS (Arrival Time Stamp: 着信時刻スタンプ) が設定されており、このタイミングはMPEG2システムズで規定されている仮想的なデコーダであるT-STD (Transport stream System Target Decoder)を破綻させないように符号化時に決定され、トランスポートストリームの再生時には、各トランスポート packetsに付加された

ATSによって出現タイミングを制御する。トランスポート・ストリーム処理手段(TS処理手段)300は、これらの制御を実行する。例えば、トランスポート packetsを記録媒体に記録する場合には、各packetの間隔を詰めたソース packetとして記録するが、各トランスポート packetsの出現タイミングを併せて記録媒体に保存することにより、再生時に各packetの出力タイミングを制御することが可能となる。トランスポート・ストリーム処理手段(TS処理手段)300は、DVD等の記録媒体195へのデータ記録時に、各トランスポート packetsの入力タイミングを表すATS (Arrival Time Stamp: 着信時刻スタンプ) を付加して記録する。

【0070】本発明の記録再生装置100は、上述のATSの付加されたトランスポートストリームによって構成されるコンテンツについて、暗号処理手段150において暗号化処理を実行し、暗号化処理のなされたコンテンツを記録媒体195に格納する。さらに、暗号処理手段150は、記録媒体195に格納された暗号化コンテンツの復号処理を実行する。これらの処理の詳細については、後段で説明する。

【0071】秘密情報復号処理手段500は、記録媒体195に格納された特殊な再生処理により読み取り可能な秘密情報の再生、復号処理を実行する処理手段である。記録媒体195に格納される秘密情報は、例えばディスクの製造磁のスタンパー毎に設定されるスタンパーID、ディスク毎に異なって設定されるディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキー等、様々な識別データ、暗号処理鍵等である。

【0072】秘密情報復号処理手段500は、記録媒体195に格納された秘密情報を読み取り復号し、復号した秘密情報を暗号処理手段150に転送する。暗号処理手段150は、秘密情報を用いて記録媒体に対するコンテンツ記録、再生時に適用する暗号処理鍵を生成する。秘密情報復号処理手段500において復号された秘密情報は記録再生装置外部からの読み取り可能な記憶手段への格納処理を行わず、暗号処理手段150内で実行されるコンテンツ暗号化キー生成においてのみ使用される構成であり、秘密情報の外部への漏洩を防止した構成となっている。

【0073】なお、図1に示す暗号処理手段150、TS処理手段300、秘密情報復号処理手段500は、理解を容易にするため、別ブロックとして示してあるが、各機能を実行する1つまたは複数のLSIとして構成してもよく、また、各機能のいずれかをソフトウェアまたはハードウェアを組み合わせた構成によって実現する構成としてもよい。

【0074】本発明の記録再生装置の構成例としては図1に示す構成の他に図2に示す構成が可能である。図2に示す記録再生装置200では、記録媒体205はドラ

イブ装置としての記録媒体インタフェース(I/F) 210から着脱が可能であり、この記録媒体205を別の記録再生装置に装着してもデータの読出し、書きこみが可能な構成としたものである。

【0075】[データ記録処理およびデータ再生処理]次に、図1あるいは図2の記録再生装置における記録媒体に対するデータ記録処理および記録媒体からのデータ再生処理について、図3および図4のフローチャートを参照して説明する。外部からのデジタル信号のコンテンツを、記録媒体195に記録する場合においては、図3(A)のフローチャートにしたがった記録処理が行われる。即ち、デジタル信号のコンテンツ(デジタルコンテンツ)が、例えば、IEEE(Institute of Electric and Electronics Engineers)1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS301において、入出力I/F120は、供給されるデジタルコンテンツを受信し、バス110を介して、TS処理手段300に出力する。

【0076】TS処理手段300は、ステップS302において、トランスポートストリームを構成する各トランスポートパケットにATSを付加したブロックデータを生成して、バス110を介して、暗号処理手段150に出力する。

【0077】暗号処理手段150は、ステップS303において、受信したデジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス110を介して、ドライブ190、あるいは記録媒体I/F210に出力する。暗号化コンテンツは、ドライブ190、あるいは記録媒体I/F210を介して記録媒体195に記録(S304)され、記録処理を終了する。なお、暗号処理手段150における暗号処理については後段で説明する。

【0078】なお、IEEE1394シリアルバスを介して接続した装置相互間で、デジタルコンテンツを伝送するときの、デジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む5社によって、5CDTCP(Five Company Digital Transmission Content Protection)(以下、適宜、DTCPという)が定められているが、このDTCPでは、コピーフリーでないデジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、デジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたデジタルコンテンツ(暗号化コンテンツ)を復号するようになっている。

【0079】このDTCPに規格に基づくデータ送受信においては、データ受信側の入出力I/F120は、ステップS301で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、DT

CPに規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段150に出力する。

【0080】DTCPによるデジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたデジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたデジタルコンテンツを、そこに含まれるキーを用いて復号する。

【0081】なお、DTCPによれば、正確には、キーの初期値と、デジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含まれる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、DTCPについては、例えば、<http://www.dtcp.com>のURL(Uniform Resource Locator)で特定されるWebページにおいて、インフォメショナルバージョン(Informational Version)の取得が可能である。

【0082】次に、外部からのアナログ信号のコンテンツを、記録媒体195に記録する場合の処理について、図3(B)のフローチャートに従って説明する。アナログ信号のコンテンツ(アナログコンテンツ)が、入出力I/F140に供給されると、入出力I/F140は、ステップS321において、そのアナログコンテンツを受信し、ステップS322に進み、内蔵するA/D、D/Aコンバータ141でA/D変換して、デジタル信号のコンテンツ(デジタルコンテンツ)とする。

【0083】このデジタルコンテンツは、MPEGコーデック130に供給され、ステップS323において、MPEGエンコード、すなわちMPEG圧縮による符号化処理が実行され、バス110を介して、暗号処理手段150に供給される。

【0084】以下、ステップSS324、S325、S326において、図3(A)のステップS302、S303における処理と同様の処理が行われる。すなわち、TS処理手段300によるトランスポートパケットに対するATS付加、暗号処理手段150における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体195に記録して、記録処理を終了する。

【0085】次に、記録媒体195に記録されたコンテンツを再生して、デジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図4のフローに従って説明する。デジタルコンテンツとして外部に出力する処理は図4(A)のフローチャートにしたがった再生処理として実行される。即ち、まず最初に、ス

テップS401において、ドライブ190または記録媒体I/F210によって、記録媒体195に記録された暗号化コンテンツが読み出され、バス110を介して、暗号処理手段150に出力される。

【0086】暗号処理手段150では、ステップS402において、ドライブ190または記録媒体I/F210から供給される暗号化コンテンツが復号処理され、復号データがバス110を介して、TS処理手段300に出力される。

【0087】TS処理手段300は、ステップS403 10において、トランスポートストリームを構成する各トランスポートパケットのATSから出力タイミングを判定し、ATSに応じた制御を実行して、バス110を介して、入出力I/F120に供給する。入出力I/F120は、TS処理手段300からのデジタルコンテンツを、外部に出力し、再生処理を終了する。なお、TS処理手段300の処理、暗号処理手段150におけるデジタルコンテンツの復号処理については後述する。

【0088】なお、入出力I/F120は、ステップS404で、IEEE1394シリアルバスを介してデジタルコ 20ンテンツを出力する場合には、DTCPPの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、デジタルコンテンツを暗号化して伝送する。

【0089】記録媒体195に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図4(B)のフローチャートに従った再生処理が行われる。

【0090】即ち、ステップS421、S422、S423において、図4(A)のステップS401、S402、S403における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段150において得られた復号されたデジタルコンテンツは、バス110を介して、MPEGコーデック130に供給される。

【0091】MPEGコーデック130では、ステップS424において、デジタルコンテンツがMPEGデコード、すなわち伸長処理が実行され、入出力I/F140に供給される。入出力I/F140は、ステップS424において、MPEGコーデック130でMPEGデコードされたデジタルコンテンツを、内蔵するA/D、D/Aコンバータ141でD/A変換(S425)して、アナログコンテンツとする。そして、ステップS426に進み、入出力I/F140は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

【0092】[データフォーマット]次に、図5を用いて、本発明における記録媒体上のデータフォーマットを説明する。本発明における記録媒体上のデータの読み書きの最小単位をブロック(block)という名前で呼ぶ。1ブロックは、 $192 \times X$ (エックス) バイト (例えば $X=32$) の大きさとなっている。

【0093】本発明では、MPEG2のTS (トランスポート・ストリーム) パケット (188バイト) にATSを付加して192バイトとして、それをX個集めて1ブロックのデータとしている。ATSは24乃至32ビットの着信時刻を示すデータであり、先にも説明したようにArrival Time Stamp (着信時刻スタンプ) の略である。ATSは各パケットの着信時刻に応じたランダム性のあるデータとして構成される。記録媒体のひとつのブロック (セクタ) には、ATSを付加したTS (トランスポート・ストリーム) パケットをX個記録する。本発明の構成では、トランスポートストリームを構成する各ブロックの第1番目のTSパケットに付加されたATSを用いてそのブロック (セクタ) のデータを暗号化するブロックキーを生成する。

【0094】ランダム性のあるATSを用いて暗号化用のブロックキーを生成することにより、ブロック毎に異なる固有キーが生成される。生成されたブロック固有キーを用いてブロック毎の暗号化処理を実行する。また、ATSを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

【0095】なお、図5に示すブロック・シード (Block Seed) は、ATSを含む付加情報である。ブロック・シードは、さらにATSだけでなくコピー制御情報 (CCI: Copy Control Information) も付加した構成としてもよい。この場合、ATSとCCIを用いてブロックキーを生成する構成とすることができる。

【0096】なお、ここで、ブロック・シードに含まれるコピー制限情報 (CCI: Copy Control Information) は、後段で説明するが、企業5社の共同提案としての5CDTCP (Digital Transmission Content Protection) システムで提唱するコピー制御情報 (CCI: Copy Control Information) であり、デバイスの能力に応じた2種類の情報、すなわち、EMI (Encryption Mode Indicator)、あるいは、コピー制御情報を送るための場所があらかじめ確保されているようなフォーマットにおいて適用されるコンテンツに埋め込まれたコピー制御情報 (CCI) である埋め込みCCI (Embedded CCI) のいずれかの情報を反映したものとなる。

【0097】なお、本発明の構成においては、DVD等の記録媒体上にデータを格納する場合、コンテンツの大部分のデータは暗号化されるが、図5の最下段に示すように、ブロックの先頭のm (たとえば、 $m=8$ または 16) バイトは暗号化されずに平文 (Unencrypted data) のまま記録され、残りのデータ ($m+1$ バイト以降) が暗号化される。これは暗号処理が8バイト単位としての処理であるために暗号処理データ長 (Encrypted data) 50

に制約が発生するためである。なお、もし、暗号処理が8バイト単位でなく、たとえば1バイト単位で行なえるなら、 $m=4$ として、ブロックシード以外の部分をすべて暗号化してもよい。

【0098】[TS処理手段における処理] ここで、ATSの機能について詳細に説明する。ATSは、先にも説明したように入力トランスポートストリーム中の各トランスポートパケットの出現タイミングを保存するために付加する着信時刻スタンプである。

【0099】すなわち、例えば複数のTVプログラム(コンテンツ)が多重化されたトランスポートストリームの中から1つまたは幾つかのTVプログラム(コンテンツ)を取り出した時、その取り出したトランスポートストリームを構成するトランスポートパケットは、不規則な間隔で現れる(図7(a)参照)。トランスポートストリームは、各トランスポートパケットの出現タイミングに重要な意味があり、このタイミングはMPEG2システムズ(ISO/IEC 13818-1)で規定されている仮想的なデコーダであるT-STD(Transport stream System Target Decoder)を破綻させないように符号化時に決定される。

【0100】トランスポートストリームの再生時には、各トランスポートパケットに付加されたATSによって出現タイミングが制御される。従って、記録媒体にトランスポートパケットを記録する場合には、トランスポートパケットの入力タイミングを保存する必要があり、トランスポートパケットをDVD等の記録媒体に記録する時に、各トランスポートパケットの入力タイミングを表すATSを付加して記録する。

【0101】図6に、デジタルインタフェース経由で入力されるトランスポートストリームをDVD等の記録媒体であるストレージメディアに記録する時のTS処理手段300において実行する処理を説明するブロック図を示す。端子600からは、デジタル放送等のデジタルデータとしてトランスポートストリームが入力される。図1または図2においては、入出力I/F120を介して、あるいは入出力I/F140、MPEGコーデック130を介して端子600からトランスポートストリームが入力される。

【0102】トランスポートストリームは、ビットストリームパーサ(parser)602に入力される。ビットストリームパーサ602は、入力トランスポートストリームの中からPCR(Program Clock Reference)パケットを検出する。ここで、PCRパケットとは、MPEG2システムズで規定されているPCRが符号化されているパケットである。PCRパケットは、100msec以内の時間間隔で符号化されている。PCRは、トランスポートパケットが受信側に到着する時刻を27MHzの精度で表す。

【0103】そして、27MHz PLL 603におい

て、記録再生器が持つ27MHzクロックをトランスポートストリームのPCRにロック(Lock)させる。タイムスタンプ発生回路604は、27MHzクロックのクロックのカウント値に基づいたタイムスタンプを発生する。そして、ブロック・シード(Block seed)付加回路605は、トランスポートパケットの第1バイト目がスミージングバッファ606へ入力される時のタイムスタンプをATSとして、そのトランスポートパケットに付加する。

【0104】ATSが付加されたトランスポートパケットは、スミージングバッファ606を通して、端子607から、暗号処理手段150に出力され、後段で説明する暗号処理が実行された後、ドライブ190(図1)、記録媒体I/F210(図2)を介してストレージメディアである記録媒体195に記録される。

【0105】図7は、入力トランスポートストリームが記録媒体に記録される時の処理の例を示す。図7(a)は、ある特定プログラム(コンテンツ)を構成するトランスポートパケットの入力を示す。ここで横軸は、ストリーム上の時刻を示す時間軸である。この例ではトランスポートパケットの入力は、図7(a)に示すように不規則なタイミングで現れる。

【0106】図7(b)は、ブロック・シード(Block Seed)付加回路605の出力を示す。ブロック・シード(Block Seed)付加回路605は、トランスポートパケット毎に、そのパケットのストリーム上の時刻を示すATSを含むブロック・シード(Block Seed)を付加して、ソースパケットを出力する。図7(c)は記録媒体に記録されたソースパケットを示す。ソースパケットは、図7(c)に示すように間隔を詰めて記録媒体に記録される。このように間隔を詰めて記録することにより記録媒体の記録領域を有効に使用できる。

【0107】図8は、記録媒体195に記録されたトランスポートストリームを再生する場合のTS処理手段300の処理構成ブロック図を示している。端子800からは、後段で説明する暗号処理手段において復号されたATS付きのトランスポートパケットが、ブロック・シード(Block seed)分離回路801へ入力され、ATSとトランスポートパケットが分離される。タイミング発生回路804は、再生器が持つ27MHzクロック805のクロックカウンタ値に基づいた時間を計算する。

【0108】なお、再生の開始時において、一番最初のATSが初期値として、タイミング発生回路804にセットされる。比較器803は、ATSとタイミング発生回路804から入力される現在の時刻を比較する。そして、タイミング発生回路804が発生する時間とATSが等しくなった時、出力制御回路802は、そのトランスポートパケットをMPEGコーデック130またはデジタル入出力I/F120へ出力する。

【0109】図9は、入力AV信号を記録再生器100

のMPEGコーデック130においてMPEGエンコードして、さらにTS処理手段300においてトランスポートストリームを符号化する構成を示す。従って図9は、図1または、図2におけるMPEGコーデック130とTS処理手段300の両処理構成を併せて示すブロック図である。端子901からは、ビデオ信号が入力されており、それはMPEGビデオエンコーダ902へ入力される。

【0110】MPEGビデオエンコーダ902は、入力ビデオ信号をMPEGビデオストリームに符号化し、それをバッファビデオストリームバッファ903へ出力する。また、MPEGビデオエンコーダ902は、MPEGビデオストリームについてのアクセスユニット情報を多重化スケジューラ908へ出力する。ビデオストリームのアクセスユニットとは、ピクチャであり、アクセスユニット情報とは、各ピクチャのピクチャタイプ、符号化ビット量、デコードタイムスタンプである。ここで、ピクチャタイプは、I/P/Bピクチャ (picture) の情報である。また、デコードタイムスタンプは、MPEG2システムズで規定されている情報である。

【0111】端子904からは、オーディオ信号が入力されており、それはMPEGオーディオエンコーダ905へ入力される。MPEGオーディオエンコーダ905は、入力オーディオ信号をMPEGオーディオストリームに符号化し、それをバッファ906へ出力する。また、MPEGオーディオエンコーダ905は、MPEGオーディオストリームについてのアクセスユニット情報を多重化スケジューラ908へ出力する。オーディオストリームのアクセスユニットとは、オーディオフレームであり、アクセスユニット情報とは、各オーディオフレームの符号化ビット量、デコードタイムスタンプである。

【0112】多重化スケジューラ908には、ビデオとオーディオのアクセスユニット情報が入力される。多重化スケジューラ908は、アクセスユニット情報に基づいて、ビデオストリームとオーディオストリームをトランスポートパケットに符号化する方法を制御する。多重化スケジューラ908は、内部に27MHz精度の基準時刻を発生するクロックを持ち、そして、MPEG2で規定されている仮想的なデコーダモデルであるT-ST Dを満たすようにして、トランスポートパケットのパケット符号化制御情報を決定する。パケット符号化制御情報は、パケット化するストリームの種類とストリームの長さである。

【0113】パケット符号化制御情報がビデオパケットの場合、スイッチ976はa側になり、ビデオストリームバッファ903からパケット符号化制御情報により指示されたペイロードデータ長のビデオデータが読み出され、トランスポートパケット符号化器909へ入力される。

【0114】パケット符号化制御情報がオーディオパケットの場合、スイッチ976はb側になり、オーディオストリームバッファ906から指示されたペイロードデータ長のオーディオデータが読み出され、トランスポートパケット符号化器909へ入力される。

【0115】パケット符号化制御情報がPCRパケットの場合、トランスポートパケット符号化器909は、多重化スケジューラ908から入力されるPCRを取り込み、PCRパケットを出力する。パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケット符号化器909へは何も入力されない。

【0116】トランスポートパケット符号化器909は、パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケットを出力しない。それ以外の場合、パケット符号化制御情報に基づいてトランスポートパケットを生成し、出力する。したがって、トランスポートパケット符号化器909は、間欠的にトランスポートパケットを出力する。到着 (Arrival) タイムスタンプ (time stamp) 計算手段910は、多重化スケジューラ908から入力されるPCRに基づいて、トランスポートパケットの第1バイト目が受信側に到着する時刻を示すATSを計算する。

【0117】多重化スケジューラ908から入力されるPCRは、MPEG2で規定されるトランスポートパケットの10バイト目の受信側への到着時刻を示すので、ATSの値は、PCRの時刻から10バイト前のバイトが到着する時刻となる。

【0118】ブロック・シード (Block Seed) 付加回路911は、トランスポートパケット符号化器909から出力されるトランスポートパケットにATSを付加する。ブロック・シード (Block seed) 付加回路911から出力されるATS付きのトランスポートパケットは、スムージングバッファ912を通して、暗号処理手段150へ入力され、後段で説明する暗号処理が実行された後、ストレージメディアである記録媒体195へ格納される。

【0119】記録媒体195へ格納されるATS付きのトランスポートパケットは、暗号処理手段150で暗号化される前に図7(c)に示すように間隔を詰めた状態で入力され、その後、記録媒体195に格納される。トランスポートパケットが間隔を詰めて記録されても、ATSを参照することによって、そのトランスポートパケットの受信側への入力時刻を制御することができる。

【0120】ところで、ATSの大きさは32ビットに決まっているわけではなく、24ビット乃至31ビットでも構わない。ATSのビット長が長いほど、ATSの時間カウンターが一周する周期が長くなる。例えば、ATSが27MHz精度のバイナリカウンターである場合、24-bit長のATSが一周する時間は、約0.6

秒である。この時間間隔は、一般のトランスポートストリームでは十分な大きさである。なぜなら、トランスポートストリームのパケット間隔は、MPEG 2の規定により、最大0.1秒と決められているからである。しかしながら、十分な余裕を見て、ATSを24-bit以上にしても良い。

【0121】このように、ATSのビット長を様々な長さとした場合、ブロックデータの付加データであるブロックシードの構成としていくつかの構成が可能となる。ブロック・シードの構成例を図10に示す。図10の例1は、ATSを32ビット分使用する例である。図10の例2は、ATSを30ビットとし、コピー制御情報(CCI)を2ビット分使用する例である。コピー制御情報は、それが付加されたデータのコピー制御の状態を表す情報であり、SCMS: Serial Copy Management SystemやCGMS: Copy Generation Management Systemが有名である。これらのコピー制御情報では、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー(Copy Free)、1世代のみのコピーを許可する1世代コピー許可(One Generation Copy Allowed)、コピーを認めないコピー禁止(Copy Prohibited)などの情報が表せる。

【0122】図10に示す例3は、ATSを24ビットとし、CCIを2ビット使用し、さらに他の情報を6ビット使用する例である。他の情報としては、たとえばこのデータがアナログ出力される際に、アナログ映像データのコピー制御機構であるマクロビジョン(Macrovision)のオン/オフ(On/Off)を示す情報など、様々な情報を利用することが可能である。

【0123】[キー配布構成としてのツリー(木)構造について]次に、図1または図2に示した記録再生装置が、データを記録媒体に記録、もしくは記録媒体から再生する際に必要なマスターキーを、各機器に配布する構成について説明する。図11は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図11の最下段に示すナンバ0~15が個々の記録再生装置である。すなわち図11に示す木(ツリー)構造の各葉(リーフ: leaf)がそれぞれの記録再生装置に相当する。

【0124】各デバイス0~15は、製造時(出荷時)に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵(ノードキー)および各リーフのリーフキーを自身で格納する。図11の最下段に示すK0000~K1111が各デバイス0~15にそれぞれ割り当てられたリーフキーであり、最上段のKRから、最下段から2番目の節(ノード)に記載されたキー: KR~K1111をノードキーとする。

【0125】図11に示すツリー構成において、例えばデバイス0はリーフキーK0000と、ノードキー: K

000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図11のツリーにはデバイスが0~15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【0126】また、図11のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばDVD、CD、MD、メモリスティック(商標)等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図11に示すキー配布構成が適用されている。

【0127】これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図11の点線で囲んだ部分、すなわちデバイス0、1、2、3を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図11の点線で囲んだ部分、すなわちデバイス0、1、2、3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図11のツリー中に複数存在する。

【0128】なお、ノードキー、リーフキーは、ある1つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【0129】このツリー構成において、図11から明らかなように、1つのグループに含まれる3つのデバイス0、1、2、3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス0、1、2、3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス0、1、2、3のみが共通のマスターキーの

設定が可能である。また、新たなマスターキーKmasterをノードキーK00で暗号化した値Enc(K00, Kmaster)を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Kmaster)を解いてマスターキー: Kmasterを得ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号化したデータであることを示す。

【0130】また、ある時点tにおいて、デバイス3の
10 所有する鍵: K0011, K001, K00, K0, KRが
攻撃者(ハッカー)により解析されて露呈したことが発
覚した場合、それ以降、システム(デバイス0, 1,
2, 3のグループ)で送受信されるデータを守るため
に、デバイス3をシステムから切り離す必要がある。そ
のためには、ノードキー: K001, K00, K0, KR
をそれぞれ新たな鍵K(t)001, K(t)00, K
(t)0, K(t)Rに更新し、デバイス0, 1, 2に
その更新キーを伝える必要がある。ここで、K(t)a
a aは、鍵K a a aの世代(Generation): tの更新キ
ーであることを示す。

【0131】更新キーの配布処理について説明する。キー
の更新は、例えば、図12(A)に示す有効化キーブ
ロック(EKB: Enabling Key Block)と呼ばれるブロッ
クデータによって構成されるテーブルをたとえばネット
ワーク、あるいは記録媒体に格納してデバイス0, 1,
2に供給することによって実行される。

【0132】図12(A)に示す有効化キーブロック
(EKB)には、ノードキーの更新に必要なデバイスの
みが更新可能なデータ構成を持つブロックデータとして
30 構成される。図12の例は、図11に示すツリー構造中
のデバイス0, 1, 2において、世代tの更新ノードキ
ーを配布することを目的として形成されたブロックデ
ータである。図11から明らかなように、デバイス0, デ
バイス1は、更新ノードキーとしてK(t)00, K
(t)0, K(t)Rが必要であり、デバイス2は、更
新ノードキーとしてK(t)001, K(t)00, K
(t)0, K(t)Rが必要である。

【0133】図12(A)のEKBに示されるようにE
KBには複数の暗号化キーが含まれる。最下段の暗号化
40 キーは、Enc(K0010, K(t)001)であ
る。これはデバイス2の持つリーフキーK0010によ
って暗号化された更新ノードキーK(t)001であ
り、デバイス2は、自身の持つリーフキーによってこの
暗号化キーを復号し、K(t)001を得ることができ
る。また、復号により得たK(t)001を用いて、図
12(A)の下から2段目の暗号化キーEnc(K
(t)001, K(t)00)を復号可能となり、更新
ノードキーK(t)00を得ることができる。以下順
次、図12(A)の上から2段目の暗号化キーEnc

(K(t)00, K(t)0)を復号し、更新ノードキ
ーK(t)0、図12(A)の上から1段目の暗号化キ
ーEnc(K(t)0, K(t)R)を復号しK(t)
Rを得る。一方、デバイス0, 1は、ノードキーK00
0は更新する対象に含まれておらず、更新ノードキーと
して必要なのは、K(t)00, K(t)0, K(t)
Rである。デバイス0, 1は、図12(A)の上から3
段目の暗号化キーEnc(K000, K(t)00)を
復号しK(t)00、を取得し、以下、図12(A)の
上から2段目の暗号化キーEnc(K(t)00, K
(t)0)を復号し、更新ノードキーK(t)0、図1
2(A)の上から1段目の暗号化キーEnc(K(t)
0, K(t)R)を復号しK(t)Rを得る。このよう
にして、デバイス0, 1, 2は更新した鍵K(t)Rを
得ることができる。なお、図12(A)のインデックス
は、復号キーとして使用するノードキー、リーフキーの
絶対番地を示す。

【0134】図11に示すツリー構造の上位段のノード
キー: K0, KRの更新が不要であり、ノードキーK0
0のみの更新処理が必要である場合には、図12(B)
の有効化キーブロック(EKB: Enabling Key Block)
を用いることで、更新ノードキーK(t)00をデバイ
ス0, 1, 2に配布することができる。

【0135】図12(B)に示すEKBは、例えば特定
のグループにおいて共有する新たなマスターキーを配布
する場合に利用可能である。具体例として、図11に点
線で示すグループ内のデバイス0, 1, 2, 3がある記
録媒体を用いており、新たな共通のマスターキーK
(t)masterが必要であるとする。このとき、デバイス
0, 1, 2, 3の共通のノードキーK00を更新したK
(t)00を用いて新たな共通の更新マスターキー: K
(t)masterを暗号化したデータEnc(K(t), K
(t)master)を図12(B)に示すEKBとともに配
布する。この配布により、デバイス4など、その他のグ
ループの機器においては復号されないデータとしての配
布が可能となる。

【0136】すなわち、デバイス0, 1, 2はEKBを
処理して得たK(t)00を用いて上記暗号文を復号す
れば、t時点でのマスターキーK(t)masterを得るこ
40 とが可能になる。

【0137】[EKBを使用したマスターキーの配布]
図13に、t時点でのマスターキーK(t)masterを得
る処理例として、K(t)00を用いて新たな共通のマ
スターキーK(t)masterを暗号化したデータEnc
(K(t)00, K(t)master)と図12(B)に示
すEKBとを記録媒体を介して受領したデバイス0の処
理を示す。

【0138】図13に示すように、デバイス0は、記録
媒体に格納されている世代: t時点のEKBと自分があ
50 らかじめ格納しているノードキーK000を用いて上述

したと同様のEKB処理により、ノードキー $K(t)0$ を生成する。さらに、復号した更新ノードキー

$(t)00$ を用いて更新マスターキー $K(t)$ masterを復号して、後にそれを使用するために自分だけが持つリーフキー $K0000$ で暗号化して格納する。なお、デバイス0が更新マスターキー $K(t)$ masterを安全に自身内に格納できる場合、リーフキー $K0000$ で暗号化する必要はない。

【0139】また、この更新マスターキーの取得処理を図14のフローチャートにより説明する。なお、記録再生装置は出荷時にその時点で最新のマスターキー： K

(c) masterを与えられ、自身のメモリに安全に（具体的にはたとえば、自身のリーフキーで暗号化して）格納しているものとする。

【0140】更新マスターキー $K(n)$ masterとEKBの格納された記録媒体が、記録再生装置にセットされると、まず最初に、ステップS1401において、記録再生装置は、記録媒体から、記録媒体に格納されているマスターキー $K(n)$ masterの時点（世代）番号： n （これを、プレ（pre-recording）記録世代情報（Generation# n ）と呼ぶことにする）を読み出す。記録媒体には、予め、マスターキー $K(n)$ masterの時点（世代）番号： n が記憶されている。また、自身が保持している暗号化マスターキー C を読み出し、ステップS1402において、その暗号化マスターキーの世代： c と、プレ記録世代情報Generation# n が表す世代： n とを比較して、その世代の前後を判定する。

【0141】ステップS1402において、プレ記録世代情報Generation# n が表す世代： n の方が、自身のメモリに記憶された暗号化マスターキー C の世代： c よりも後でない（新しくない）と判定された場合、即ち、メモリに記憶された暗号化マスターキー C の世代： c が、プレ記録世代情報Generation# n が表す世代： n と同一か、または後の場合、ステップS1403乃至S1408をスキップして、マスターキー更新処理を終了する。即ち、この場合、自身のメモリに記憶されたマスターキー $K(c)$ master（暗号化マスターキー C ）の更新は行う必要がないので、その更新は行われない。

【0142】一方、ステップS1402において、プレ記録世代情報Generation# n が表す世代： n の方が、メモリに記憶された暗号化マスターキー C の世代： c よりも後である（新しい）と判定された場合、即ち、メモリに記憶された暗号化マスターキー C の世代が、プレ記録世代情報Generation# n が表す世代 n よりも前の世代である場合、ステップS1403に進み、記録再生装置は、記録媒体から、有効化キーブロック（EKB：Enabling Key Block）を読み出す。

【0143】ステップS1404において、記録再生装置は、ステップS1403で読み出したEKBと、自身がメモリに格納しているリーフキー（図11のデバイス

0における $K0000$ ）およびノードキー（図11のデバイス0における $K000, K00...$ ）を用いて、プレ記録世代情報Generation# n （図13における t ）時点でのノード00の鍵 $K(t)00$ を計算する。

【0144】ステップS1405では、ステップS1404において $K(t)00$ を得られたか否かを検査する。得られなかった場合は、その時点においてその記録再生装置がツリー構成のグループからリボーク（排除）されていることを示すので、ステップS1406乃至S1408をスキップしてマスターキー更新処理を終了する。

【0145】 $K(t)00$ を得られた場合、ステップS1406に進み、記録媒体から $Enc(K(t)00, K(t) master)$ 、すなわち、 $K(t)00$ を用いて t 時点でのマスターキーを暗号化した値を読み出す。そしてステップS1407において、この暗号文を $K(t)00$ を用いて復号して $K(t) master$ を計算する。

【0146】ステップS1408では、自身のみが持つリーフキー（図11のデバイス0における $K0000$ ）を用いて $K(t) master$ を暗号化してメモリに格納する。以上で、マスターキーの更新処理が完了する。

【0147】ところで、マスターキーは、時点（世代）0から昇順に使用されていくが、新しい世代のマスターキーから、古い世代のマスターキーを計算によりシステム内の各機器が求められる構成とすることが望ましい。すなわち、記録再生装置は、一方向性関数 f を保持しており、その一方向性関数 f に、自身が持つマスターキーを、そのマスターキーの世代と、必要なマスターキーの世代との差に対応する回数だけ適用することにより、調べた世代のマスターキーを作成する。

【0148】具体的には、例えば、記録再生装置に記憶されているマスターキー MK の世代が世代 $i+1$ であり、あるデータの再生に必要な（記録時に使用された）マスターキー MK の世代が世代 $i-1$ である場合、マスターキー $K(i-1) master$ は、記録再生装置において、一方向性関数 f が2回用いられ、 $f(f(K(i+1) master))$ を計算することにより生成される。

【0149】また、記録再生装置に記憶されているマスターキーの世代が世代 $i+1$ であり、必要なマスターキーの世代が世代 $i-2$ である場合、マスターキー $K(i-2) master$ は、一方向性関数 f を3回用いて、 $f(f(f(K(i+1) master)))$ を計算することにより生成される。

【0150】ここで、一方向性関数としては、例えば、ハッシュ(hash)関数を用いることができる。具体的には、例えば、MD5(Message Digest 5)や、SHA-1(Secure Hash Algorithm - 1)等を採用することができる。キーを発行するキー発行機関は、これらの一方向性関数を用いて自身の世代より前の世代を生成可能なマスターキー $K(0) master, K(1) master, K(2) ma$

ster . . . , K (N) masterを、あらかじめ求めておく。即ち、まず最初に、第N世代のマスターキーK

(N) masterを設定し、そのマスターキーK (N) masterに、一方向性関数を1回ずつ適用していくことで、それより前の世代のマスターキーK (N-1) master, K (N-2) master, . . . , K (1) master, K (0) masterを順次生成しておく。そして、世代の小さい(前の)マスターキーK (0) masterから順番に使用していく。なお、自身の世代より前の世代のマスターキーを生成するのに用いる一方向性関数は、すべての記録再生装置に設定されているものとする。

【0151】また、一方向性関数としては、例えば、公開鍵暗号技術を採用することも可能である。この場合、キー発行機関は、公開鍵暗号方式の秘密鍵を所有し、その秘密鍵に対する公開鍵を、すべての再生装置に与えておく。そして、キー発行機関は、第0世代のマスターキーK (0) masterを設定し、そのマスターキーK (0) masterから使用していく。即ち、キー発行機関は、第1世代以降のマスターキーK (i) masterが必要になったら、その1世代前のマスターキーK (i-1) masterを、秘密鍵で変換することにより生成して使用する。この場合、キー発行機関は、一方向性関数を用いて、N世代のマスターキーを、あらかじめ生成しておく必要がない。また、この方法によれば、理論上は、無制限の世代のマスターキーを生成することができる。なお、記録再生装置では、ある世代のマスターキーを有していれば、そのマスターキーを、公開鍵で変換することにより、その世代より前の世代のマスターキーを得ることができる。

【0152】次に、この記録再生装置がコンテンツを自身の記録媒体に記録する場合の、記録再生装置の処理について図15のフローチャートを用いて説明する。コンテンツデータは、ある世代のマスターキーにより暗号化されてネットワークあるいは記録媒体を介してコンテンツプロバイタから各記録再生装置に配布される。

【0153】まず最初に、ステップS1501において、記録再生装置は、記録媒体から、プレ記録世代情報Generation#nを読み出す。また、自身のメモリが記憶している暗号化マスターキーCの世代cを取得し、ステップS1502において、その暗号化マスターキーの世代cと、プレ記録世代情報Generation#nが表す世代nとを比較して、その世代の前後を判定する。

【0154】ステップS1502において、メモリに記憶された暗号化マスターキーCの世代cが、プレ記録世代情報Generation#nが表す世代n以後でないと判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代cが、プレ記録世代情報Generation#nが表す世代nよりも古い世代である場合、ステップS1503をスキップして、すなわち、コンテンツデータの記録処理を行わずに終了する。

【0155】一方、ステップS1502において、自身の記録再生装置内のメモリに記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation#nが表す世代n以後であると判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation#nが表す世代nと同一か、またはそれよりも新しい場合、ステップS1503に進み、コンテンツデータの記録処理を行う。

【0156】[世代管理のなされたマスターキーによるコンテンツデータ暗号化および記録処理] 以下、世代管理のなされたマスターキーによってコンテンツデータの暗号化処理を実行して、自己の記録媒体に格納する処理について説明する。なお、ここでは、先に説明したトランスポートストリームによって構成されるデータを世代管理されたマスターキーを利用したデータに基づいてブロックキーを生成してブロックキーによりコンテンツデータを暗号化して記録媒体に格納する処理について説明する。

【0157】図16、図17の処理ブロック図および図18のフローチャートを用いて説明する。ここでは、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータのbit-by-bitコピーを防ぐために、記録媒体固有の識別情報としてのディスクID(Disc ID)を、データを暗号化する鍵に作用させるようにしている。

【0158】図16、図17の処理ブロック図に従って、暗号処理手段150が実行するデータの暗号化処理の概要について説明する。

【0159】記録再生装置1600は自身のメモリ180(図1、2参照)に格納しているマスターキー1601、データ解析記録方式用キー(コグニザントキー: Cognizant Key)1631もしくはデータ非解析記録方式用キー(ノンコグニザントキー: Non-Cognizant Key)1632を読み出す。データ解析記録方式用キー(Cognizant Key)、データ非解析記録方式用キー(Non-Cognizant Key)については、後述する。

【0160】マスターキー1601は、図14のフローにより記録再生装置のメモリに格納された秘密キーであり、前述のように世代管理がなされており、それぞれに世代番号が対応付けられている。このマスターキーは、複数の記録再生装置に共通なキー、例えば図11に示す点線枠のグループに属するデバイスに共通なキーである。デバイスIDは記録再生装置1600の識別子であり、予め記録再生装置に格納されている例えば製造番号等の識別子である。このデバイスIDは公開されていてもよい。データ解析記録方式用キー(Cognizant Key)1631、データ非解析記録方式用キー(Non-Cognizant Key)1632は、それぞれの記録モードに対応したキーであり、複数の記録再生装置に共通のキーである。これらは予め記録再生装置1600のメモリに格納され

ている。

【0161】記録再生装置1600は例えば光ディスクである記録媒体1620に識別情報としてのディスクID (Disc ID) 1603が既に記録されているかどうかを検査する。記録されていれば、ディスクID (Disc ID) 1603を読み出し(図16に相当)、記録されていなければ、暗号処理手段150においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法でディスクID (Disc ID) 1701を生成し、ディスクに記録する(図17に相当)。ディスクID (Disc ID) 1603はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

【0162】記録再生器1600は、次にマスターキーと、特殊な読み取り方法でのみディスクから読み取り可能な秘密情報として記録されたスタンパーID (Stamper ID) 1680と、ディスクID 1603を用いて、ディスク固有キー (Disc Unique Key) を生成1602する。

【0163】マスターキーと秘密情報としてのスタンパーID (Stamper ID) 1680とディスクID 1603とを用いディスク固有キー (Disc Unique Key) の具体的な生成方法としては、図19に示すように、ブロック暗号関数を用いたハッシュ関数にマスターキー (Master Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) を入力して得られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとスタンパーID (Stamper ID) とディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用する例2の方法が適用できる。

【0164】上述したように、スタンパーID (Stamper ID) 1680は、あらかじめディスクに記録されている高度な秘密情報であり、その読み出しおよび読み出されたスタンパーID (Stamper ID) を利用したディスク固有キー (Disc Unique Key) の生成などの演算処理は、秘密が保たれるように暗号処理手段内部で実行される。すなわち、ディスクから読み出された秘密情報は暗号処理手段内においてセキュアに保護される。

【0165】このように、本発明の構成においては、特殊な読み出し方法でのみ読み取り可能な秘密情報は、正当なデバイス、すなわち秘密情報の読み取り方法を実行可能なデバイスでのみ読み取られ、たとえばLSI内に実装されて高度に保護された暗号鍵の生成を実行する暗号処理部においてセキュアな保護の下にコンテンツ暗号処理用の鍵生成処理に使用される構成であり、秘密情報が外部からの読み取り可能なメモリ上に格納されない。従って、秘密情報の漏洩の可能性がなく、不正なコンテンツの再生処理を効果的に防止することが可能となる。

【0166】上述したように、スタンパーID等の秘密

情報は、通常のデータ書き込み手法とは異なる態様でディスクに書き込まれ、また、通常のデータ読み出しとは異なる手法でのみ読み取り可能である。この秘密情報の書き込みおよび読み出し処理構成例については後段で詳細に説明する。

【0167】記録再生装置1600は、次に、記録ごとの固有鍵であるタイトルキー (Title Key) を暗号処理手段150 (図1, 2, 参照) においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法で生成1604し、ディスク1620に記録する。

【0168】さらに、この記録における記録モードがデータ解析記録方式 (Cognizant Mode) かデータ非解析記録方式 (Non-cognizant) かを表すフラグを設定1633し、ディスク1620に記録モード1635を記録する。

【0169】ここで、データ解析記録方式 (Cognizant Mode) およびデータ非解析記録方式 (Non-Cognizant Mode) について説明する。

【0170】コンテンツはそれぞれあらかじめコンテンツ提供者によっていかなる条件で複製が可能かを指定されている。そこで、ネットワーク接続においてもその指定された条件を正しく相手の機器に伝える必要性があり、企業5社の共同提案としての5C D T C P (Digital Transmission Content Protection) システムではコピー制御情報 (CCI : Copy Control Information) という方法を用いて解決している。コピー制御情報 (CCI) はデバイスの能力に応じて2種類の伝達方法が規定されている。

【0171】エンクリプションモード・インディケータ (EMI : Encryption Mode Indicator) はパケットヘッダにあるSyビットの上位2ビットを使ってコピー制御情報 (CCI) を送るメカニズムであり、受信デバイスが簡単にアクセスする事ができると同時に、この値がコンテンツを暗号化する鍵に作用するため安全に送ることができるようになっている。

【0172】EMIによりそのパケットの暗号化モードを示し、コンテンツ暗号・復号鍵の生成モードを指定する。EMIをIEEE1394パケットヘッダに置くことにより、受信機器は例えばMPEG転送ストリーム (MPEG transport stream) の中に埋め込まれている埋め込みコピー制御情報 (Embedded CCI) (後述) を取り出すことなく簡単にどのモードでコンテンツが暗号化されているかを知ることができる。

【0173】図20にIEEE1394パケットフォーマットを示す。データフィールド (Data Field) 中には、音楽データ、画像データ等、様々なコンテンツが格納され、コピー制御情報 (CCI) としてのエンクリプション・モード・インディケータ (EMI : Encryption Mode Indicator) はパケットヘッダにあるSyビットの上位2ビットに設定される。

【0174】EMIの2ビット情報は、設定値に応じてコンテンツの異なる取り扱いを規定する。具体的には、値00は認証も暗号化も必要がなく、コンテンツは自由にコピーが可能なコピーフリー (Copy Free) を示し、値01は一代コピーの作成が可能なコピー1ジェネレーション (Copy One Generation) を、値10は前述のCopy One Generation が一度記録された後の、再コピーが禁止されているノーモアコピー (No More Copies) を、値11はコンテンツがリリース時点からコピー禁止であるネバーコピー (Never Copy) を表す。

【0175】D-VHSやハードディスクのような記録されるデータのフォーマットを認識しないようなビットストリームレコーダでも正しく著作物を取り扱えるように、記録時に埋め込みCCI (Embedded CCI) の更新 (e x. Copy One Generationから No More Copiesへ) を必要とせず、EMIの更新のみ行えばよい、という記録方法がデータ非解析 (Non-Cognizant) 記録方式である。

【0176】一方、こういったコピー制御情報を送るための場所があらかじめ確保されているようなフォーマット (たとえばDVフォーマット: DV-format) においては、CCIはコンテンツの一部として伝送することができる。このように、コンテンツの一部としてコンテンツに埋め込まれたコピー制御情報 (CCI) を埋め込みCCI (Embedded CCI) と呼ぶ。通常、コンテンツが暗号化されて転送される場合、埋め込みCCI (Embedded CCI) もコンテンツと同様に暗号化されて転送され、埋め込みCCI (Embedded CCI) の故意の変更は困難とされている。

【0177】ここで、前述したEMIの2ビットのコピー制御情報と、埋め込みCCI (Embedded CCI) との双方を持つコンテンツの場合、コンテンツ記録を実行するある記録デバイスは、EMIおよび埋め込みCCI (Embedded CCI) の双方のコピー制御情報の更新を行なう。しかし、埋め込みCCI (Embedded CCI) の解析能力のない記録デバイスの場合、EMIは更新するが、埋め込みCCI (Embedded CCI) の更新は実行しないことになる。

【0178】コンテンツ記録時に、記録デバイスがコンテンツの一部として伝送された埋め込みCCI (Embedded CCI) の更新を行ってコンテンツとともに記録する記録方式をデータ解析 (Cognizant) 記録方式という。データ解析 (Cognizant) 記録方式と、データ非解析 (Non-Cognizant) 記録方式では、データ非解析 (Non-Cognizant) 記録方式の方が埋め込みCCI (Embedded CCI) の更新を行わなくてよい分、負荷が軽く実装しやすいが、5C D T C Pのルールとして、その機器がコンテンツをM P E Gデコードしてアナログ端子から映像信号を表示するためにはその機器はデータ解析記録方式 (Cognizant Mode) でなければならないというルールがあり、デコー

ド/表示機能を持つ機器はデータ解析記録方式 (Cognizant Mode) を実行する機能を備えていることが必要である。

【0179】しかしまた、データ解析記録方式 (Cognizant Mode) を実行するためには、コンテンツの一部として埋め込まれている埋め込みCCI (Embedded CCI) の位置や意味を完全に知る必要があり、たとえばある機器が市場に出た後に制定された新規のあるいは更新されたデータフォーマットについては、その新しいデータフォーマットに対して、古い機器がデータ解析記録方式 (Cognizant Mode) を実行するのは非常に困難となる場合がある。

【0180】従って、コンテンツを記録するある機器が、特定のデータフォーマットについては、もしくは、特定の機能を実現するときには、データ解析記録方式 (Cognizant Mode) を実行し、また異なるデータフォーマットのコンテンツ記録時には、データ非解析記録方式 (Non-Cognizant Mode) を実行するといった、両方の記録方式を実行することが考えられる。

【0181】また、すべてのコンテンツに対して、データ非解析記録方式 (Non-Cognizant Mode) の記録しか行わない機器も存在する。また、逆に埋め込みCCI (Embedded CCI) を理解できるフォーマットを持つコンテンツの処理しか実行しない機器、すなわちデータ解析記録方式 (Cognizant Mode) のみ実行する機器も存在することが考えられる。

【0182】このように、2つのコピー制御情報、すなわちEMIと埋め込みCCI (Embedded CCI) が存在し、またコンテンツ記録を実行する機器としても、データ解析記録方式 (Cognizant Mode) を実行する機器と、データ非解析記録方式 (Non-Cognizant Mode) の記録を実行する機器が混在する状況においては、データ解析記録方式 (Cognizant Mode) で記録したコンテンツと、データ非解析記録方式 (Non-Cognizant Mode) で記録したコンテンツは明確に区別されることが好ましい。

【0183】すなわち、データ解析記録方式 (Cognizant Mode) でコンテンツを記録した場合にはEMIも埋め込みCCI (Embedded CCI) の双方のコピー制御情報が更新されるが、データ非解析記録方式 (Non-Cognizant Mode) でコンテンツの記録が実行された場合は、EMIのみが更新され、埋め込みCCI (Embedded CCI) の更新が行なわれない。その結果、記録媒体上のEMIと埋め込みCCI (Embedded CCI) に不整合がおり、その両者が混ざると混乱が生じるためである。従って、2つのコピー制御情報の不整合を発生させないためには、データ解析記録方式 (Cognizant Mode) で記録されたコンテンツは、データ解析記録方式 (Cognizant Mode) モードでの記録再生処理を実行し、データ非解析記録方式 (Non-Cognizant Mode) で記録されたコンテンツはデータ非解析記録方式 (Non-Cognizant Mode) モードで記録

再生処理を実行する構成とすることが必要となる。

【0184】このためには、このデータ解析記録方式 (Cognizant Mode) と、データ非解析記録方式 (Non-Cognizant Mode) とをまったく別の記録方式とすることも一案ではあるが、この場合、1つの機器において両方のモードを選択的に実行可能とするためには、1機器に両モードの実行処理構成を装備することが必要となり、これは、機器のコスト高を招くという問題がある。

【0185】そこで本発明の構成では、この2つの記録方式、すなわちデータ解析記録方式 (Cognizant Mode) と、データ非解析記録方式 (Non-Cognizant Mode) のいずれの方式を適用するかに応じて、コンテンツ暗号処理の鍵を異なる鍵として生成して使用する構成とすることで、機器および記録方式に応じて2つの記録方式を明確に区別して、両方式が無秩序に混在して実行される事態を解消し、機器および記録方式に応じたいずれか一方の統一的な記録方式によるコンテンツ処理構成を、機器の装備および処理負荷を増大させることなく実現したものである。

【0186】具体的には、データ解析記録方式 (Cognizant Mode) 記録用の秘密情報 (再生時にも必要) としての暗号化、復号処理鍵生成用のキー (データ解析記録方式用キー (Cognizant Key)) をデータ解析記録方式 (Cognizant Mode) による記録または再生を行える機能を持つ機器にのみ提供して機器内に格納する構成とし、一方、データ非解析記録方式 (Non-Cognizant Mode) 記録用の秘密情報 (再生時にも必要) としての暗号化、復号処理鍵生成用のキー (データ非解析記録方式用キー (Non-Cognizant Key)) を、データ非解析記録方式 (Non-Cognizant Mode) による記録または再生を行える機能を持つ機器にのみ提供して機器内に格納する構成とした。

【0187】本構成により、例えば、データ解析記録方式 (Cognizant Mode) で記録されたコンテンツについて、バグを原因として、あるいはデータの改竄、記録再生プログラムの不正改造等によって、データ非解析記録方式 (Non-Cognizant Mode) の記録再生機能のみを有する機器において、誤ってまたは不正な記録再生の実行を防止することができる。

【0188】図16、図17に戻って、コンテンツ記録処理の説明を続ける。記録再生装置1600は、さらに、使用するマスターキーの世代番号、すなわち、自身が格納するマスターキーの世代番号 [記録時世代番号 (Generation#n)] 1650を取得して、これを記録媒体1620に記録時世代番号1651として格納する。

【0189】ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー1605、記録モードフラグ1635、マスターキーの世代番号 [記録時世代番号 (Generation#n)] 1651を格納することができる。

【0190】なお、記録媒体1620には、予め、プレ (pre-recording) 世代番号が格納されており、プレ世代番号と同一またはプレ世代番号より新しい世代のマスターキーを用いて暗号化されて格納されたコンテンツのみの再生を可能とする構成となっている。この構成については、後段の再生処理の欄で説明する。

【0191】次にディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key)、あるいは、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ非解析記録方式用キー (Non-Cognizant Key)、いずれかの組合せから、タイトル固有キー (Title Unique Key) を生成する。

【0192】すなわち、記録モードがデータ解析記録方式 (Cognizant Mode) である場合には、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) とからタイトル固有キー (Title Unique Key) を生成し、記録モードがデータ非解析記録方式 (Non-Cognizant Mode) である場合には、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ非解析記録方式用キー (Non-Cognizant Key) とからタイトル固有キー (Title Unique Key) を生成する。

【0193】前述したように、データ解析記録方式 (Cognizant Mode) 記録用の秘密情報としての暗号化、復号処理鍵生成用のキー (データ解析記録方式用キー (Cognizant Key)) は、データ解析記録方式 (Cognizant Mode) による記録または再生を行える機能を持つ機器のみが有し、一方、データ非解析記録方式 (Non-Cognizant Mode) 記録用の秘密情報としての暗号化、復号処理鍵生成用のキー (データ非解析記録方式用キー (Non-Cognizant Key)) は、データ非解析記録方式 (Non-Cognizant Mode) による記録または再生を行える機能を持つ機器のみが有する。従って、一方の記録方式にのみ対応した機器においては、いずれか一方のモードのみを選択してコンテンツ記録が実行される。すなわち、データ解析記録方式用キー (Cognizant Key) を用いるか、あるいはデータ非解析記録方式用キー (Non-Cognizant Key) を用いるかの一方のみに限られることとなる。

【0194】しかし、両者のキーを格納し、両モードの記録方式を実行可能な機器においては、いずれのモードによる記録を実行するかを決定する処理が必要となる。このモード決定プロセス処理について、すなわち、コンテンツの記録をデータ解析記録方式 (Cognizant Mode) によって実行するか、データ非解析記録方式 (Non-Cognizant Mode) で実行するかを決定するプロセスについて図21を用いて説明する。

【0195】基本的には、コンテンツ記録は、できる限りデータ解析記録方式 (Cognizant Mode) によって実行するのが望ましい。これは、前述したように、EMI と埋

め込みCCI (Embedded CCI) との不整合を生じさせないためである。ただし、前述したように、新規なデータフォーマットの出現等によるデータ解析エラー等の発生の可能性もあり、このような場合に、データ非解析記録方式 (Non-Cognizant Mode)での記録処理を実行する。

【0196】図21の各ステップについて説明する。ステップS5001では、記録装置は、データ・フォーマットを解析可能か否かを判定する。先に説明したように、埋め込みCCI (Embedded CCI) は、コンテンツの内部に埋め込まれており、データフォーマットの解析が不可能であれば、埋め込みCCI (Embedded CCI) の読み取りが不可能となるので、この場合は、データ非解析記録方式 (Non-Cognizant Mode)での記録処理を実行する。

【0197】データフォーマットの解析が可能であれば、ステップS5002に進み、記録装置が、データ (コンテンツ) のデコード処理、埋め込みCCI (Embedded CCI) の読み取り、更新処理が可能か否かを判定する。コンテンツおよび埋め込みCCI (Embedded CCI) は通常、符号化 (エンコード) されており、埋め込みCCI (Embedded CCI) の読み取りには復号 (デコード) を実行することが必要となる。例えば多チャンネル同時記録などの際に、復号回路が他に使用されているなど理由で、機器が復号処理可能でない場合は、埋め込みCCI (Embedded CCI) の読み取りができないので、データ非解析記録方式 (Non-Cognizant Mode)での記録処理を実行する。

【0198】ステップS5002のデータ (コンテンツ) のデコード処理、埋め込みCCI (Embedded CCI) の読み取り、更新処理が可能であると判定されると、ステップS5003において、記録装置に対するユーザ入力中に、データ非解析モードでの記録処理の実行指定入力があるか、否かが判定される。この処理は、ユーザの指定によるモード選択を可能とした機器においてのみ実行されるステップであり、通常の機器、すなわちユーザによるモード指定を許容しない機器においては実行されない。ユーザ入力によるデータ非解析記録方式 (Non-Cognizant Mode)での記録処理指定があった場合は、データ非解析記録方式 (Non-Cognizant Mode)での記録処理が実行される。

【0199】次に、ステップS5004において、コンテンツパケット (ex. 受信データ) 中に、データ非解析モードでの記録処理の実行指定があるか否かが判定される。データ中にデータ非解析モードでの記録処理の実行指定がある場合は、データ非解析記録方式 (Non-Cognizant Mode)での記録処理が実行される。指定がない場合は、データ解析記録方式 (Cognizant Mode)での記録処理が実行される。

【0200】データ解析記録方式 (Cognizant Mode)での記録処理、およびデータ非解析記録方式 (Non-Cognizant Mode)での記録処理の双方を選択的に実行可能な機器においては、上述したモード決定プロセス処理によって、いずれのモードでの記録を実行するかが決定される。ただし、図21の処理フローからも理解されるように、データ解析記録方式 (Cognizant Mode)での記録が可能な場合は、基本的にデータ解析記録方式 (Cognizant Mode)での処理が実行されることになる。

【0201】前述したように、記録モードをデータ解析記録方式 (Cognizant Mode)とした場合は、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) からタイトル固有キー (Title Unique Key) を生成し、記録モードをデータ非解析記録方式 (Non-Cognizant Mode)とした場合は、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ非解析記録方式用キー (Non-Cognizant Key) とからタイトル固有キー (Title Unique Key) を生成する。

【0202】タイトル固有キー (Title Unique Key) 生成の具体的な方法を図22に示す。図22に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー (Title Key) とディスク固有キー (Disc Unique Key) と、データ解析記録方式用キー (Cognizant Key) (データ解析記録方式 (Cognizant Mode)の場合)、もしくは、データ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode)の場合)を入力して得られた結果を用いる例1の方法、あるいは、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID (Disc ID) とデータ解析記録方式用キー (Cognizant Key) (データ解析記録方式 (Cognizant Mode)の場合)もしくはデータ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode)の場合)とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをタイトル固有キー (Title Unique Key) として使用する例2の方法が適用できる。

【0203】なお、上記の説明では、マスターキー (Master Key) とスタンパーID (Stamper ID)とディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) とデータ解析記録方式用キー (Cognizant Key)もしくはデータ非解析記録方式用キー (Non-Cognizant Key)からタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてマスターキー (Master Key) とディスクID (Disc ID) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key)もしくはデータ非解析記録方式用キー (Non-Cognizant Key)から直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、マ

10

20

30

40

50

スターキー (Master Key) とディスク ID (Disc ID) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

【0204】たとえば上記の5CDTCPに規定される伝送フォーマットのひとつを使用した場合、データはMPEG2のTSパケットで伝送される場合がある。たとえば、衛星放送を受信したセットトップボックス (STB: Set Top Box) がこの放送を記録機に5CDTCPを用いて伝送する際に、STBは衛星放送通信路で伝送されたMPEG2 TSパケットをIEEE1394上も伝送することが、データ変換の必要がなく望ましい。

【0205】記録再生装置1600は記録すべきコンテンツデータをこのTSパケットの形で受信し、前述したTS処理手段300において、各TSパケットを受信した時刻情報であるATSを付加する。なお、先に説明したように、ブロックデータに付加されるブロック・シードは、ATSとコピー制御情報、さらに他の情報を組み合わせた値から構成してもよい。

【0206】ATSを付加したTSパケットをX個 (例えばX=32) 並べて、1ブロックのブロックデータが形成 (図5の上の図参照) され、図16、17の下段に示すように、被暗号化データとして入力されるブロックデータの先頭の第1~4バイトが分離され (セクタ1608) て出力される32ビットのATSを含むブロックシード (Block Seed) と、先に生成したタイトル固有キー (Title Unique Key) とから、そのブロックのデータを暗号化する鍵であるブロック・キー (Block Key) が生成1607される。

【0207】ブロック・キー (Block Key) の生成方法の例を図23に示す。図23では、いずれも32ビットのブロック・シード (Block Seed) と、64ビットのタイトル固有キー (Title Unique Key) とから、64ビットのブロックキー (Block Key) を生成する例を2つ示している。

【0208】上段に示す例1は、鍵長64ビット、入出力がそれぞれ64ビットの暗号関数を使用している。タイトル固有キー (Title Unique Key) をこの暗号関数の鍵とし、ブロックシード (Block Seed) と32ビットの定数 (コンスタント) を連結した値を入力して暗号化した結果をブロックキー (Block Key) としている。

【0209】例2は、FIPS 180-1のハッシュ関数SHA-1を用いた例である。タイトル固有キー (Title Unique Key) とブロックシード (Block Seed) を連結した値をSHA-1に入力し、その160ビットの出力を、たとえば下位64ビットのみ使用するなど、64ビットに縮約したものをブロックキー (Block Key) としている。

【0210】なお、上記ではディスク固有キー (Disc U

nique key)、タイトル固有キー (Title Unique Key)、ブロックキー (Block Key) をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー (Disc Unique Key) とタイトル固有キー (Title Unique Key) の生成を実行することなく、ブロックごとにマスターキー (Master Key) とスタンプID (Stamper ID) とディスクID (Disc ID) とタイトルキー (Title Key) とブロックシード (Block Seed) と、データ解析記録方式用キー (Cognizant Key) (Cognizant Mode の場合) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode) の場合) を用いてブロックキー (Block Key) を生成してもよい。

【0211】ブロックキーが生成されると、生成されたブロックキー (Block Key) を用いてブロックデータを暗号化する。図16、17の下段に示すように、ブロックシード (Block Seed) を含むブロックデータの先頭の第1~mバイト (たとえばm=8) は分離 (セクタ1608) されて暗号化対象とせず、m+1バイト目から最終データまでを暗号化1609する。なお、暗号化されないmバイト中にはブロック・シードとしての第1~4バイトも含まれる。セクタ1608により分離された第m+1バイト以降のブロックデータは、暗号処理手段150に予め設定された暗号化アルゴリズムに従って暗号化1609される。暗号化アルゴリズムとしては、たとえばFIPS 46-2で規定されるDES (Data Encryption Standard) を用いることができる。

【0212】また、前述したようにブロック・シードには、コピー制限情報 (CCI: Copy Control Information) を含ませることが可能であり、データ解析記録方式 (Cognizant Mode) での記録処理を実行した場合には、コンテンツデータ内部に埋め込まれたコピー制御情報 (CCI) である埋め込みCCI (Embedded CCI) に対応するコピー制御情報が記録され、また、データ非解析記録方式 (Non-Cognizant Mode) での記録処理を実行した場合には、図20で説明したパケットヘッダ上のEMI (Encryption Mode Indicator) を反映したコピー制御情報が記録される。

【0213】すなわち、データ解析記録方式 (Cognizant Mode) による情報記録処理の場合、データ部内の埋め込みコピー制御情報 (CCI) に基づくコピー制御情報を含むブロックシードを、1以上のパケットからなるブロックデータに付加した記録情報生成処理を実行し、データ非解析記録方式 (Non-Cognizant Mode) による情報記録処理の場合、パケットに含まれるコピー制御情報としてのエンクリプション・モード・インディケータ (EMI) に基づくコピー制御情報を含むブロックシードを、1以上のパケットからなるブロックデータに付加した記録情報生成処理を実行する。

【0214】ここで、使用する暗号アルゴリズムのプロ

ック長（入出力データサイズ）がDESのように8バイトであるときは、Xを例えば32とし、mを例えば8の倍数とすることで、端数なくm+1バイト目以降のブロックデータ全体が暗号化できる。

【0215】すなわち、1ブロックに格納するTSパケットの個数をX個とし、暗号アルゴリズムの入出力データサイズをLバイトとし、nを任意の自然数とした場合、 $192 \times X = m + n \times L$ が成り立つようにX、m、Lを定めることにより、端数処理が不要となる。

【0216】暗号化した第m+1バイト以降のブロックデータは暗号処理のされていない第1～mバイトデータとともにセクタ1610により結合されて暗号化コンテンツ1612として記録媒体1620に格納される。

【0217】以上の処理により、コンテンツはブロック単位で、世代管理されたマスターキー、ATSを含むブロック・シード等に基づいて生成されるブロック鍵で暗号化が施されて記録媒体に格納される。

【0218】上述のように、本構成では、世代管理されたマスターキーによりコンテンツデータが暗号化され記録媒体に格納されているので、その記録媒体を他の記録再生器における再生処理は、少なくとも同一世代、あるいはデータを記録した際に使用されたマスターキーの世代より新しい世代を有する記録再生器であることが復号、すなわち再生可能となる条件となる。

【0219】さらに、ブロックキーは上述のようにデータ解析記録方式 (Cognizant Mode) の記録の場合は、データ解析記録方式用キー (Cognizant Key) に基づいて生成され、データ非解析記録方式 (Non-Cognizant Mode) の記録の場合は、データ非解析記録方式用キー (Non-Cognizant Key) に基づいて生成される。これらの暗号化データは、記録時と同一のモードに対応する鍵（データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key)）を持つ機器でのみ再生可能となる。

【0220】すなわち、データ解析記録方式用キー (Cognizant Key) は、記録時にストリーム中に埋め込まれた Embedded CCI を認識して必要に応じて更新する能力を持つ機器およびそのデータの再生を許された機器にのみ与えられ、この鍵を持たない機器ではデータ解析記録方式 (Cognizant Mode) で記録されたコンテンツの再生は行えない。

【0221】同様に、データ非解析記録方式用キー (Non-Cognizant Key) は、記録時にストリーム中の埋め込み CCI (Embedded CCI) を認識しないデータ非解析記録方式 (Non-Cognizant) の記録モードの機能を持つ機器と、そのモードで記録されたデータの再生を許された機器にのみ与えられ、この鍵を持たない機器ではデータ非解析記録方式 (Non-Cognizant Mode) で記録されたコンテンツの再生は行えないようになっている。なお、再生処理の詳細については後述する。

【0222】次に図18に示すフローチャートに従って、データ記録処理にともなって実行されるTS処理手段300におけるATS付加処理および暗号処理手段150における暗号処理の処理全体の流れをまとめて説明する。図18のS1801において、記録再生装置は自身のメモリ180に格納しているマスターキーおよびデータ解析記録方式用キー (Cognizant Key) (データ解析記録方式 (Cognizant Mode) の場合) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode) の場合) を読み出す。また、ディスクからスタンパーID (Stamper ID) を読み出す。

【0223】S1802において、記録媒体に識別情報としてのディスクID (Disc ID) が既に記録されているかどうかを検査する。記録されていればS1803でこのディスクIDを読み出し、記録されていなければS1804で、ランダムに、もしくはあらかじめ定められた方法でディスクIDを生成し、ディスクに記録する。次に、S1805では、マスターキーとスタンパーID (Stamper ID) とディスクIDを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用することで求める。

【0224】次にS1806に進み、その一回の記録ごとの固有の鍵としてのタイトルキー (Title Key) を生成し、記録モード (Recording Mode) とマスターキーの世代番号とともにディスクに記録する。記録モード (Recording Mode) は、実行する情報記録モードが、データ解析記録方式 (Cognizant Mode) であるか、データ非解析記録方式 (Non-Cognizant Mode) であるかを示す。

【0225】次にS1807で、上記のディスク固有キーとタイトルキーと、データ解析記録方式用キー (Cognizant Key) (データ解析記録方式 (Cognizant Mode) の場合) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode) の場合) から、タイトル固有キーを生成する。

【0226】タイトル固有キーの生成の詳細フローを図24に示す。暗号処理手段150は、ステップS2001において、記録モードにより分岐する。この分岐は、記録再生器のプログラムや、記録再生器を使用するユーザによって入力された指示データに基づいて判定される。

【0227】S2001で記録モードがデータ解析記録方式 (Cognizant Mode)、すなわち、Cognizant 記録の場合は、ステップS2002に進み、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) とから、タイトル固有キー (Title Unique Key) を生成する。

【0228】S2001で記録モードがデータ非解析記

録方式 (Non-Cognizant Mode)、すなわち、Non-Cognizant 記録の場合は、ステップS2003に進みディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ非解析記録方式用キー (Non-Cognizant Key) とから、タイトル固有キー (Title Unique Key) を生成する。キー生成には、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

【0229】S1808では、記録再生装置は記録すべきコンテンツデータの被暗号化データをTSパケットの形で受信する。S1809で、TS処理手段300は、各TSパケットを受信した時刻情報であるATSを付加する。あるいはコピー制御情報CCIとATS、さらに他の情報を組み合わせた値を付加する。次に、S1810で、ATSを付加したTSパケットを順次受信し、1ブロックを形成する例えばX=32に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップS1811に進み、X個、あるいはパケット終了までのパケットを並べて、1ブロックのブロックデータを形成する。

【0230】次に、暗号処理手段150は、S1812で、ブロックデータの先頭の32ビット (ATSを含むブロック・シード) とS1807で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

【0231】S1813では、ブロックキーを用いてS1811で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのm+1バイト目から最終データまでである。暗号化アルゴリズムは、たとえばFIPS 46-2で規定されるDES (Data Encryption Standard) が適用される。

【0232】S1814で、暗号化したブロックデータを記録媒体に記録する。S1815で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければS1808に戻って残りのデータの処理を実行する。

【0233】上述の処理にしたがって、コンテンツの記録処理がデータ解析記録方式 (Cognizant Mode) あるいは、データ非解析記録方式 (Non-Cognizant Mode) のいずれかによって実行される。コンテンツの記録処理がデータ解析記録方式 (Cognizant Mode) で実行される場合は、コンテンツの暗号化に適用される鍵が、データ解析記録方式用キー (Cognizant Key) に基づいて生成され、また、コンテンツの記録処理がデータ非解析記録方式 (Non-Cognizant Mode) で実行される場合は、コンテンツの暗号化に適用される鍵がデータ非解析記録方式用キー (Non-Cognizant Key) に基づいて生成されることになる。従って、それぞれの方式においてディスクに記録されたコンテンツは、記録時に使用したデータ解析記録方

式用キー (Cognizant Key)、あるいはデータ非解析記録方式用キー (Non-Cognizant Key) のいずれか、同一のキーを適用して復号用の鍵を生成することが必須となり、各方式が混在した記録、再生処理が防止される。

【0234】[秘密情報の書き込みおよび再生] 次に、図16、図17等にしたスタンプID等の秘密情報を、通常の方法書き込み手法とは異なる態様でディスクに書き込み、また、通常の方法読み出しとは異なる手法を適用した場合にのみ読み取り可能な態様とした秘密情報の書き込みおよび読み出し処理構成例について説明する。

【0235】(信号の擾乱による秘密情報生成) まず、スタンプID等の各種情報信号をM系列信号により擾乱して記録する構成について説明する。

【0236】図25に秘密情報の書き込み処理のための書き込み信号生成変調回路構成を示す。図25に示す変調回路は、データ書き込み対象であるディスク原盤が、所定の角度だけ回転する毎に信号レベルが立ち上がるFG信号を基準にしてスタンプID等の秘密情報の変調を行ない書き込みを実行する。

【0237】PLL回路1041は、FG信号を基準にディスク原盤の回転に同期したチャンネルクロックCKを生成して変調回路の各部に供給する。

【0238】タイミングジェネレータ1042は、チャンネルクロックCKをカウントすることにより、所定の時間間隔でM系列発生回路1045A~1045Dを初期化する初期化パルスSYを発生する。また、タイミングジェネレータ1042は、初期化パルスSYに同期した同期パターン選択信号STを生成して出力する。

【0239】図25に示す変調回路においては、チャンネルクロックCKに対して格段に遅いビットレートでスタンプID等の秘密情報が入力される。同期パターン発生回路1043は、初期化パルスSYの立上がりを基準にして所定の同期パターンDYを生成して出力する。

【0240】M系列発生回路1045a~1045Dは、初期化パルスSYにより初期化され、チャンネルクロックCK単位で変化するM系列M1~M4を出力する。ここでM系列M1~M4は、ランダムに論理値が変化し、かつ論理1と論理0との発生確率が等確立であるデータ列であり、相互に無相関である。

【0241】演算回路(X)1046A~1046Dは、エクスクルーシブオア回路により構成され、それぞれM系列信号M1~M4と、スタンプID、ディスクID等の秘密情報の各ビットb0~b3とエクスクルーシブオア演算を実行して演算結果を出力する。これにより、スタンプID等の秘密情報は、M系列信号M1~M4により擾乱される。

【0242】乱数発生回路1047は、2ビットの乱数(0, 1, 2, 3のいずれかの値)RをチャンネルクロックCK単位で発生し、データセクタ1048に出力す

る。データセクタ1048は、乱数Rの値に応じて演算回路1046A~1046Dの演算結果を選択出力する。例えば乱数R=0のとき演算回路1046Aの出力選択、乱数R=1のとき演算回路1046Bの出力選択、乱数R=2のとき演算回路1046Cの出力選択、乱数R=3のとき演算回路1046Dの出力選択とする。

【0243】この構成により、変調回路は、対応するM系列M1~M4を基準にした復号により他の演算結果による影響を受けずに1046A~1046Dの演算結果を1系統としてさらに擾乱する構成を可能としている。 10

【0244】データセクタ1049は、同期パターン信号STを基準にして同期パターン発生回路1043から出力される同期パターンDY、データセクタ1048の出力を選択出力する。これにより、初期化パルスSYが立ち上がった後、所定のクロック周期、例えば5クロック周期の間同期パターン[ex. 11011]の後、データセクタ1048の出力を行なう。

【0245】ディスク原盤には、所定の秘密情報書き込み領域に図25に示す変調回路において生成された出力が書き込まれる。変調回路に入力されるスタンパーID等の秘密情報が同一でも、乱数に応じて書き込みデータ態様が異なることになる。従って通常の読み出し処理においては解析困難なデータの書き込みが可能となる。 20

【0246】次に、上述の手法で書き込まれた秘密情報の再生処理について、図26を用いて説明する。図26は、ディスクから読み取られたデジタル再生信号DXからスタンパーID等の秘密情報を復号する復号処理手段構成を示す図である。PLL回路1081は、ディスクから読み取られたデジタル再生信号DXを基準にして記録時に生成したチャネルクロックCKを再生して各部に出力する。 30

【0247】同期検出回路1082は、チャネルクロックCKを基準にしたデジタル再生信号DXの識別により同期パターンを検出し、検出結果により記録時の初期化パルスSYを再生する。M系列発生回路1083A~1083Dは、この初期化パルスSY、チャネルクロックCKを基準にして、それぞれ記録時に生成したM系列M1~M4を出力する。

【0248】乗算回路(X)1084A~1084Dは、それぞれM系列信号M1~M4とデジタル再生信号DXを乗算して乗算結果を出力する。なお、ここで乗算回路(X)1084A~1084Dは、M系列信号M1~M4の論理値に応じてデジタル再生信号DXの極性を反転することにより、この乗算処理を実行する。デジタル再生信号DXは、対応するM系列M1~M4を基準にした復号によってのみ正しく再生される。 40

【0249】積分回路1085A~1085Dは、乗算回路1084A~1084Dにより出力される乗算結果をそれぞれ初期化パルスSYを基準にして積分することにより、スタンパーID等の秘密情報の対応するビット 50

列b1~b3の論理値に応じた値の積分結果を出力する。判定回路1086A~1086Dは、それぞれ積分回路1085A~1085Dより出力される積分結果を初期化パルスSYを基準にして2値識別することにより、スタンパーID等の秘密情報の各ビットb0~b3を復号して出力する。

【0250】上述したように、スタンパーID等の秘密情報は、4ビットパラレルビット列b0~b3として変調回路(図25)に入力され、4系統のM系列M1~M4、また乱数Rによる擾乱がなされて記録されるので、通常の読み出し処理での読み取りが困難となる。また、再生時には同期パターンDYを基準にしてM系列M1~M4を生成可能となり、生成したM系列により、読み取り信号の復号により、スタンパーID等の秘密情報の出力が可能となる。

【0251】上述の記録方式により書き込まれたスタンパーIDを読み取り、スタンパーID等に基づいてコンテンツの暗号処理鍵を生成する記録再生装置は、図26の構成を持つ秘密情報復号処理手段構成を持つ。

【0252】(ディスク内周に秘密情報を記録)次に、秘密情報の書き込み、再生処理の異なる例として、音楽データ等の書き込み領域とは異なるディスク領域にスタンパーID等の秘密情報を書き込み、これをフォーカスサーボにより安定的に読み取ることを可能とした構成について説明する。

【0253】図27は、スタンパーID等の秘密情報を記録したディスクを示す斜視図である。スタンパーID等の秘密情報は、ディスクの1周に4回繰り返して記録され、部分的に損傷が発生した場合でも秘密情報の再生が可能となるように構成される。秘密情報は、ヘッダー、スタンパーID等の情報領域、さらに誤り訂正符号が割り当てられた構成を持つ。これらの情報を示すビットパターンの各ビットは、ユーザデータとして記録されるデータ領域の各ビットに比較して格段に長い、例えば50μm単位の微小領域を単位として形成される。また、スタンパーIDの情報領域、誤り訂正符号領域には、3つの微小領域の中心領域のみ、記録面の光学特性を変化させたパターンが形成された同期パターンが形成され、この同期パターンにより、再生時のタイミング制御が可能となる。

【0254】また、スタンパーID等の情報領域、誤り訂正符号領域データは、2ビット毎にデータを区切り、2ビットデータ(b1, b0)が、論理00の場合、図27(D1)に示すように、先頭の微小領域のみの記録面の光学特性を変化を発生させ、論理[1000]に変換して記録する。以下、(D2)2ビットデータ(b1, b0)が、論理01の場合、[0100]、(D3)2ビットデータ(b1, b0)が、論理10の場合、[0010]、(D4)2ビットデータ(b1, b0)が、論理11の場合、[0001]とする。これに

より、ディスク上には、光学特性の変化した領域の存在比率が0.3以下となり、ディスク内周領域においても十分な反射光量によるフォーカスサーボを可能としてデータ読み取りを可能となる。

【0255】図28は、ディスク内周領域に記録したスタンパーID等の秘密情報の読み取りに用いられる復号処理手段構成を示した図である。PLL回路1160は、デジタル再生信号DXよりチャネルクロックCKを再生出力する。

【0256】同期検出回路1161は、チャネルクロックCKを基準にしてデジタル再生信号DXの信号レベルを判定することにより、同期パターンを検出して初期化パルスSYを出力する。

【0257】タイミングジェネレータ1162は、初期化パルスSYを基準にして、同期パターンに続く図27に示す第1～4の微小領域について、それぞれ各微小領域のほぼ中央で立ち上がるサンプリングパルスT1～T4を出力する。

【0258】フリップフロップ(FF)1163A～1163Dは、それぞれサンプリングパルスT1～T4を基準にしてデジタル再生信号をラッチする。これにより、スタンパID、ディスクID等の情報領域、誤り訂正符号領域データの各2ビットに割り当てた4つの微小領域より得られる再生信号の信号レベルを、それぞれフリップフロップ1163A～1163Dにラッチして保持する。

【0259】最大値検出回路1164は、これら4つのラッチD1～D4の大小判定により、スタンパーID、ディスクID等の情報領域、誤り訂正符号領域の2ビットデータ(b1, b0)を復号して出力し、パラレルシリアル変換回路(PS)1165は、順次、最大値検出回路1164より出力される2ビットデータ(b1, b0)をシリアルデータに変換して出力する。

【0260】上述の記録方式により書き込まれたスタンパーIDを読み取り、スタンパーID等に基づいてコンテンツの暗号処理鍵を生成する記録再生装置は、図28の構成を秘密情報復号処理手段構成を持つ。

【0261】このように、コンテンツとは異なる特殊な秘密情報書き込み手法と読み取り手法の構成を採用して、スタンパーID等の秘密情報をディスクに格納し、これをコンテンツの暗号化、復号処理に適用する鍵の元データとして使用する構成としたので、たとえ他の処理鍵が漏洩したとしても、ディスクに格納されたスタンパーID等の秘密情報は読み取りが困難であり、漏洩の可能性を激減させることが可能となり、よりセキュリティを高めたコンテンツ保護が可能となる。

【0262】なお、本明細書においては、ディスクに格納する特定のデータ書き込み処理、再生処理を要求される秘密情報をスタンパーIDとして設定した例を説明するが、スタンパーIDに限らず、ディスク毎に異なって

設定されるディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキー等、様々な識別データ、暗号処理鍵をディスクに格納する秘密情報として設定することが可能である。これらの様々な秘密情報を適用してコンテンツの暗号処理鍵を生成する。

【0263】なお、上述した記録再生装置は、図16、図17に示すように、データ解析記録方式(Cognizant Mode)記録用の暗号化、復号処理鍵生成用のキー(データ解析記録方式用キー(Cognizant Key))と、データ非解析記録方式(Non-Cognizant Mode)記録用の暗号化、復号処理鍵生成用のキー(データ非解析記録方式用キー(Non-Cognizant Key))との双方を選択的に使用可能な構成であるが、いずれか一方のみの方式を実行する記録再生装置においては、いずれか一方のキー、すなわちデータ解析記録方式用キー(Cognizant Key)、あるいはデータ非解析記録方式用キー(Non-Cognizant Key)のみを格納しており、格納キーに基づいてコンテンツの暗号化、復号処理用のブロックキーを生成する。これら単独のキーを格納した記録再生装置におけるコンテンツの暗号処理鍵の生成処理過程を示すブロック図を図29、図30に示す。

【0264】図29は、データ解析記録方式用キー(Cognizant Key)のみを有する記録再生装置であり、記録媒体に対するデータ記録、記録媒体からのデータ再生の際に使用する暗号化キー、復号キーをデータ解析記録方式用キー(Cognizant Key)他のキー生成データに基づいて生成して、コンテンツの暗号化、復号を実行する構成である。

【0265】図30は、データ非解析記録方式用キー(Non-Cognizant Key)のみを有する記録再生装置であり、記録媒体に対するデータ記録、記録媒体からのデータ再生の際に使用する暗号化キー、復号キーをデータ非解析記録方式用キー(Non-Cognizant Key)他のキー生成データに基づいて生成して、コンテンツの暗号化、復号を実行する構成である。

【0266】これらの単独キー格納装置においては、いずれか一方の方式においてのみデータの記録、再生が実行可能となる。

【0267】[世代管理のなされたマスターキーによるコンテンツデータ復号および再生処理]次に、上記のようにして記録媒体に記録された暗号化コンテンツを復号して再生する処理について図31の処理ブロック図と、図32～図34のフローチャートを用いて説明する。

【0268】図31の処理ブロック図を参照しながら、図32に示すフローチャートに従って、復号処理および再生処理について、処理の流れを説明する。図32のS2401において、記録再生装置2300(図31参照)はディスク2320からディスクID2302とプレ(pre-recording)記録世代番号とスタンパーID(S

tamper ID) 2380を読み出し、また自身のメモリからマスターキー2301、データ解析記録方式用キー (Cognizant Key) 2331および/あるいはデータ非解析記録方式用キー (Non-Cognizant Key) 2332を読み出す。先の記録処理の説明から明らかなように、ディスクIDはディスクにあらかじめ記録されているか、そうでない場合は記録再生器において生成してディスクに記録したディスク固有の識別子である。

【0269】プレ (pre-recording) 記録世代番号2360は、予め記録媒体であるディスクに格納されたディスク固有の世代情報である。このプレ (pre-recording) 世代番号と、データ記録時のマスターキーの世代番号、すなわち記録時世代番号2350を比較して再生処理の可否を制御する。マスターキー2301は、図14のフローにより記録再生装置のメモリに格納され世代管理のなされた秘密キーである。データ解析記録方式用キー (Cognizant Key) およびデータ非解析記録方式用キー (Non-Cognizant Key) は、それぞれデータ解析 (Cognizant) 記録モードおよびデータ非解析 (Non-Cognizant) 記録モードに対応したシステム共通の秘密キーである。

【0270】記録再生装置2300は、次に、S2402で、ディスクから読み出すべきデータのタイトルキー、さらに、データの記録モード、データを記録したときに使用したマスターキーの世代番号 (Generation #) すなわち記録時世代番号2350を読み出す。次に、S2403で読み出すべきデータが再生可能か否かを判定する。判定の詳細フローを図33に示す。

【0271】図33のステップS2501において、記録再生装置は、S2401で読み出したプレ世代番号と、S2402で読み出した記録時世代番号の新旧を判定する。記録時世代番号が示す世代が、プレ記録世代情報が表す世代以後でないと判定された場合、即ち、データ記録時世代情報が表す世代が、プレ記録世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、ステップS2404乃至S2409をスキップして、再生処理を行わずに処理を終了する。従って、記録媒体に記録されたコンテンツが、プレ記録世代情報が表す世代よりも古い世代のマスターキーに基づいて暗号化されたものである場合には、その再生は許可されず、再生は行われない。

【0272】即ち、この処理は、不正が発覚して、最新の世代のマスターキーが与えられなくなった不正な記録装置で、古い世代のマスターキーに基づいて、データが暗号化され、記録媒体に記録された場合に該当するものと判断し、そのような不正な装置によってデータが記録された記録媒体の再生は行わないとした処理である。これにより、不正な記録装置の使用を排除することができる。

【0273】一方、ステップS2501において、記録時世代番号が表す世代が、プレ記録世代番号が表す世代

以後であると判定された場合、即ち、記録時世代情報が表す世代が、プレ記録世代番号が表す世代nと同一か、または新しい世代であり、従って、記録媒体に記録されたコンテンツが、プレ記録世代情報が表す世代以後の世代のマスターキーに基づいて暗号化されたものである場合には、ステップS2502に進み、記録再生装置は、自身のメモリが記憶している暗号化マスターキーCの世代情報を取得し、その暗号化マスターキーの世代と、暗号時世代情報が表す世代を比較して、その世代の前後を判定する。

【0274】ステップS2502において、メモリに記憶されたマスターキーCの世代が、記録時世代情報が表す世代以後でないと判定された場合、即ち、メモリに記憶されたマスターキーCの世代が、記録時世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、ステップS2404乃至S2409をスキップして、再生処理を行わずに処理を終了する。

【0275】一方、ステップS2502において、メモリに記憶された暗号化マスターキーCの世代が、記録時世代情報が表す世代以後であると判定された場合、即ち、メモリに記憶されたマスターキーCの世代が、記録時世代情報が表す世代と同一か、またはそれよりも新しい場合、ステップS2503に進み、記録時のモードに対応する鍵、すなわちデータ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) を、再生機器自身が所有しているかどうかを判断する。

【0276】ステップS2503において、記録時のモードに対応する鍵であるデータ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) を、再生機器自身が所有している場合、再生可能と判定する。記録時のモードに対応する鍵 (データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key)) を、再生機器自身が所有していない場合、再生不可能と判定する。

【0277】再生可能と判定された場合は、ステップS2404に進む。S2404では、ディスクID (Disc ID) とマスターキー (Master Key) とスタンパーID (Stamper ID) を用いてディスク固有キー (Disc Unique Key) を生成2302する。このキー生成方法は、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用する方や、ブロック暗号関数を用いたハッシュ関数にマスターキー (Master Key) とディスクID (Disc ID) を入力して得られた結果を用いるなどの方法が挙げられる。ここで使用するマスターキーは、図32のステップS2402で記録媒

体から読み出した、そのデータの記録時世代番号が表す世代（時点）のマスターキーである。もし記録再生装置がこれよりも新しい世代のマスターキーを保持している場合には、前述した方法を用いて記録時世代番号が表す世代のマスターキーを作成し、それを用いてディスク固有キー（Disc Unique Key）を生成してもよい。

【0278】次に、S2405で、タイトル固有キーの生成を行なう。タイトル固有キーの生成の詳細フローを図34に示す。暗号処理手段150は、ステップS2601において、記録モードの判定を実行する。この判定は、ディスクから読み出した記録モード（Recording Mode）に基づいて実行される。

【0279】S2601において、記録モードがデータ解析記録方式（Cognizant Mode）であると判定された場合は、ステップS2602に進み、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key）とから、タイトル固有キー（Title Unique Key）を生成する。

【0280】S2601において、記録モードがデータ非解析記録方式（Non-Cognizant Mode）であると判定された場合は、ステップS2603に進み、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ非解析記録方式用キー（Non-Cognizant Key）とから、タイトル固有キー（Title Unique Key）を生成する。キー生成には、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

【0281】なお、上記の説明では、マスターキー（Master Key）とスタンパーID（Stamper ID）とディスクID（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデータ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）からタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてマスターキー（Master Key）とスタンパーID（Stamper ID）とディスクID（Disc ID）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）から直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、マスターキー（Master Key）とスタンパーID（Stamper ID）とディスクID（Disc ID）と、データ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

【0282】次にS2406でディスクから暗号化されて格納されている暗号化コンテンツ2312から順次ブロックデータ（Block Data）を読み出し、S2407で、ブロックデータの先頭の4バイトのブロック・シー

ド（Block Seed）をセクタ2310において分離して、ブロックシード（Block Seed）と、S2405で生成したタイトル固有キーを用いてブロックキーを生成する。

【0283】ブロック・キー（Block Key）の生成方法は、先に説明した図23の構成を適用することができる。すなわち、32ビットのブロック・シード（Block Seed）と、64ビットのタイトル固有キー（Title Unique Key）とから、64ビットのブロックキー（Block Key）を生成する構成が適用できる。

【0284】なお、上記説明ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロックごとにマスターキー（Master Key）とスタンパーID（Stamper ID）とディスクID（Disc ID）とタイトルキー（Title Key）と、ブロックシード（Block Seed）と、データ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）を用いてブロックキー（Block Key）を生成してもよい。

【0285】ブロックキーが生成されると、次にS2408で、ブロックキー（Block Key）を用いて暗号化されているブロックデータを復号2309し、セクタ2308を介して復号データとして出力する。なお、復号データには、トランスポートストリームを構成する各トランスポートパケットにATSが付加されており、先に説明したTS処理手段300において、ATSに基づくストリーム処理が実行される。その後、データは、使用、たとえば、画像を表示したり、音楽を再生したりすることが可能となる。

【0286】このように、ブロック単位で暗号化され記録媒体に格納された暗号化コンテンツはブロック単位でATSを含むブロック・シードに基づいて生成されるブロック鍵で復号処理が施されて再生が可能となる。ブロックキーを用いて暗号化されているブロックデータを復号し、S2409で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければS2406に戻り残りのデータを読み出す。

【0287】なお、上述した記録再生装置は、図31に示すように、データ解析記録方式（Cognizant Mode）記録用の暗号化、復号処理鍵生成用のキー（データ解析記録方式用キー（Cognizant Key））と、データ非解析記録方式（Non-Cognizant Mode）記録用の暗号化、復号処理鍵生成用のキー（データ非解析記録方式用キー（Non-Cognizant Key））との双方を選択的に使用可能な構成例であるが、先に図29、図30に示して説明したように、いずれか一方のキー、すなわちデータ解析記録方式用キー（Cognizant Key）、あるいはデータ非解析記録

方式用キー (Non-Cognizant Key) のみを格納した機器においては、いずれか一方のみの格納キーに対応する方式のみを実行し、格納キーに基づいてコンテンツの復号処理用のブロックキーを生成する。

【0288】〔記録媒体にのみ有効なメディアキーを使用した処理構成〕ところで、上記の実施例においては、有効化キーブロック (EKB: Enabling Key Block) を用いて各記録再生装置に対してマスターキーを伝送し、これを用いて記録再生装置がデータの記録、再生を行うとしていた。

【0289】マスターキーは、その時点におけるデータの記録全体に有効な鍵であり、ある時点のマスターキーを得ることができた記録再生装置は、その時点およびそれ以前にこのシステムで記録されたデータを復号することが可能になる。ただし、システム全体で有効であるというその性質上、マスターキーが攻撃者に露呈した場合の影響がシステム全体に及ぶという不具合もある。

【0290】これに対し、記録媒体のEKB (Enabling Key Block) を用いて伝送する鍵を、全システムに有効なマスターキーではなく、その記録媒体にのみ有効なメディアキーとすることにより、キーの露呈の影響を抑えることが可能となる。以下に、第2の実施例としてマスターキーの代わりにメディアキーを用いる方式を説明する。ただし、第1の実施例との変更部分のみを説明する。

【0291】図35には、図13と同様の例として、デバイス0が記録媒体に格納されているt時点のEKBと自分があらかじめ格納しているリーフキーK0000とノードキーK000、K00を用いて更新ノードキーK(t)00を生成し、これを用いて更新メディアキー: K(t) mediaを得る様子を示している。ここで得たK(t) mediaは、その記録媒体のデータの記録、再生時に使用される。

【0292】なお、図35におけるプレ記録世代番号 (Generation #n) は、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので必須ではなくオプションとして設定される。

【0293】各記録再生装置は、たとえば、データの記録もしくは再生のために記録媒体が記録再生装置に挿入された際に、図36に示すフローチャートによってその記録媒体用のメディアキー: K(t) mediaを計算し、後にその記録媒体へのアクセスに使用する。

【0294】図36のステップS2801のEKBの読みこみとS2802のEKBの処理は、それぞれ図14のステップS1403およびS1404と同様の処理である。

【0295】ステップS2803において記録再生装置はメディアキーK(t) mediaをノードキー K(t) 00で暗号化した暗号文 Enc (K(t) 00, K(t) media) を記録媒体から読みこみ、ステップS2804で

これを復号してメディアキーを得る。もしこの記録再生装置が図11に示すツリー構成のグループから排除、すなわちリボークされていれば、メディアキーを入手できず、その記録媒体への記録および再生が行えない。

【0296】次に、記録媒体へのデータの記録の処理を説明するが、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので、第1の実施例において図15に示した、プレ記録世代情報と記録再生装置自身が格納するマスターキーの世代の比較による記録可能かどうかのチェックは行わず、上記処理においてメディアキーを得られていれば記録を行えると判断する。すなわち、図37に示す処理フローのようになる。図37の処理フローは、メディアキーの取得をS2901で判定し、取得された場合にのみ、ステップS2902においてコンテンツの記録処理を実行するものである。

【0297】〔記録媒体にのみ有効なメディアキーを使用したデータの記録処理〕コンテンツデータの記録処理の様子を、図38、39のブロック図および図40のフローチャートを用いて説明する。

【0298】本実施例では、第1の実施例と同様、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータの bit-by-bit コピーを防ぐために、記録媒体固有の識別情報としてのディスクID (Disc ID) を、データを暗号化する鍵に作用させるようにしている点も同様である。

【0299】図38および図39は、それぞれ第1の実施例における図16および図17に対応する図であり、マスターキー (Master Key) の代わりにメディアキー (Media Key) が使われている点が異なっており、また、マスターキーの世代を示す記録時代番号 (Generation #) を用いていない点が異なっている。図38および図39の差異は、図16、図17の差異と同様ディスクIDの書き込みを実行するかしないかの差異である。

【0300】図40はメディアキーを用いる本実施例におけるデータ記録処理を示すものであり、前述した図18 (実施例1) のフローチャートに対応する。以下、図40の処理フローについて実施例1と異なる点を中心として説明する。

【0301】図40のS3201において、記録再生装置3000は自身のメモリに格納しているデータ解析記録方式用キー (Cognizant Key) および/もしくはデータ非解析記録方式用キー (Non-Cognizant Key) と、図36のS2804で計算し、一時的に保存しているメディアキーK(t) mediaを読み出す。また、ディスクからスタンパーID (Stamper ID) を読み出す。

【0302】S3202において、記録再生装置は記録媒体 (光ディスク) 3020に識別情報としてのディスクID (Disc ID) が既に記録されているかどうかを検査する。記録されていれば、S3203でこのディスクID (Disc ID) を読出し (図38に相当)、記録され

10

20

30

40

50

ていなければ、S3204で、ランダムに、もしくはあらかじめ定められた方法でディスクID (Disc ID) を生成し、ディスクに記録する (図39に相当)。ディスクID (Disc ID) はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。いずれの場合でも、次にS3205に進む。

【0303】S3205では、S3201で読み出したメディアキーとスタンパーID (Stamper ID) とディスクID (Disc ID) を用いて、ディスク固有キー (Disc Unique Key) を生成する。ディスク固有キー (Disc Unique Key) の具体的な生成方法としては、第1の実施例で使用した方法と同じ方法で、マスターキーの代わりにメディアキーを使用すればよい。

【0304】次にS3206に進み、その一回の記録ごとに固有の鍵: タイトルキー (Title Key) をランダムに、あるいはあらかじめ定められた方法で生成し、ディスクに記録する。同時に、このタイトル (データ) を記録したときの記録モード (Recording Mode) をディスクに記録する。

【0305】ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー、RecordingMode を格納することができる。

【0306】ステップS3207乃至S3215は図18のS1807乃至S1815と同様であるため説明を省略する。

【0307】なお、上記の説明では、メディアキー (Media Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) とデータ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてメディアキー (Media Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) から直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、メディアキー (Media Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

【0308】以上のようにして、メディアキーを用いて記録媒体にデータを記録することができる。

【0309】[記録媒体にのみ有効なメディアキーを使用したデータの再生処理] 次に、上記のようにして記録

されたデータを再生する処理の様子を図41のブロック図と図42のフローチャートを用いて説明する。

【0310】図41は、第1の実施例における図31に対応する図であり、マスターキー (Master Key) の変わりにメディアキー (Media Key) が使われ、そのため記録時世代番号 (Generation #) が省略されている点が異なっている。

【0311】図42のS3401において、記録再生装置3400は記録媒体であるディスク3420からスタンパーID (Stamper ID) およびディスクID (Disc ID) を、また自身のメモリからデータ解析記録方式用キー (Cognizant Key) および/あるいはデータ非解析記録方式用キー (Non-Cognizant Key) と、図36のS2804で計算し一時的に保存しているメディアキーを読み出す。

【0312】なお、この記録媒体の挿入時に、図36の処理を行い、メディアキーを入手できなかった場合には、再生処理を行わずに終了する。

【0313】次にS3402で、ディスクから読み出すべきデータのタイトルキー (Title Key) とこのデータを記録した際の記録モード Recording Mode を読み出す。

【0314】次にS3403で、このデータが再生可能であるか否かを判断する。S3403の処理の詳細を図43に示す。

【0315】ステップS3501ではメディアキー (Media Key) を得られたか否かを判定する。メディアキーを得られなかった場合、再生不可能となり、メディアキーを得られた場合はステップS3502に進む。ステップS3502の処理は図33のS2503と同じであり、そのデータの記録時に使われた記録モードに対応する鍵 (データ解析記録方式 (Cognizant Mode) の場合、データ解析記録方式用キー (Cognizant Key)、データ非解析記録方式 (Non-Cognizant Mode) の場合、データ非解析記録方式用キー (Non-Cognizant Key)) を再生機器が持っている場合には「再生可能」と判断してステップS3404に進み、それ以外の場合には、「再生不可能」と判断して、ステップS3404乃至S3409をスキップして、再生処理を行わずに処理を終了する。

【0316】ステップS3404乃至S3409の処理は、図32のS2404乃至S2409と同様であるため、説明を省略する。

【0317】なお、上記の説明では、メディアキー (Media Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてメディアキー (Media Key) とスタンパ

ーID (Stamper ID)とディスクID (Disc ID) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) から直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、メディアキー (Media Key) とスタンプーID (Stamper ID)とディスクID (Disc ID) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) 相当の鍵 10 を生成してもよい。

【0318】上記のようにして、記録媒体へのデータの記録および記録媒体からの再生処理が実行される。

【0319】〔記録処理におけるコピー制御〕さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

【0320】即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしても良いもの (コピー可能) かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合に 20 は、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

【0321】そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録再生を行う場合の図1または図2の記録再生装置の処理について、図44および図45のフローチャートを参照して説明する。

【0322】まず、外部からのデジタル信号のコンテンツを、記録媒体に記録する場合においては、図44 30 (A) のフローチャートにしたがった記録処理が行われる。図44 (A) の処理について説明する。図1の記録再生器100を例として説明する。デジタル信号のコンテンツ (デジタルコンテンツ) が、例えば、IEEE1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS4001において、入出力I/F120は、そのデジタルコンテンツを受信し、ステップS4002に進む。

【0323】ステップS4002では、入出力I/F120は、受信したデジタルコンテンツが、コピー可能 40 かどうかを判定する。即ち、例えば、入出力I/F120が受信したコンテンツが暗号化されていない場合 (例えば、上述のDTCPを使用せずに、平文のコンテンツが、入出力I/F120に供給された場合) には、そのコンテンツは、コピー可能であると判定される。

【0324】また、記録再生装置100がDTCPに準拠している装置であるとし、DTCPに従って処理を実行するものとする。DTCPでは、コピーを制御するためのコピー制御情報としての2ビットのEMI (Encrypt 50

ion Mode Indicator)が規定されている。EMIが00B (Bは、その前の値が2進数であることを表す) である場合は、コンテンツがコピーフリーのもの (Copy-free ly) であることを表し、EMIが01Bである場合には、コンテンツが、それ以上のコピーをすることができないもの (No-more-copies) であることを表す。さらに、EMIが10Bである場合は、コンテンツが、1度だけコピーして良いもの (Copy-one-generation) であることを表し、EMIが11Bである場合には、コンテンツが、コピーが禁止されているもの (Copy-never) であることを表す。

【0325】記録再生装置100の入出力I/F120に供給される信号にEMIが含まれ、そのEMIが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、EMIが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

【0326】ステップS4002において、コンテンツがコピー可能でないと判定された場合、ステップS4003～S4005をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体10に記録されない。

【0327】また、ステップS4002において、コンテンツがコピー可能であると判定された場合、ステップS4003に進み、以下、ステップS4003～S4005において、図3 (A) のステップS302、S303、S304における処理と同様の処理が行われる。すなわち、TS処理手段300によるトランスポートパケットに対するATS付加、暗号処理手段150における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体195に記録して、記録処理を終了する。

【0328】なお、EMIは、入出力I/F120に供給されるデジタル信号に含まれるものであり、デジタルコンテンツが記録される場合には、そのデジタルコンテンツとともに、EMI、あるいは、EMIと同様にコピー制御状態を表す情報 (例えば、DTCPにおけるembedded CCIなど) も記録される。

【0329】この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。

【0330】本発明の記録再生装置では、このEMIやembedded CCIなどのコピー制御情報を、TSパケットに付加する形で記録する。即ち、図10の例2や例3のように、ATSを24ビットないし30ビット分と、コピー制御情報を加えた32ビットを図5に示すように各TSパケットに付加する。

【0331】外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図44 (B) のフローチャートにしたがった記録処理が行われる。図44

(B) の処理について説明する。アナログ信号のコンテンツ(アナログコンテンツ)が、入出力I/F140に供給されると、入出力I/F140は、ステップS4011において、そのアナログコンテンツを受信し、ステップS4012に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

【0332】ここで、ステップS4012の判定処理は、例えば、入出力I/F140で受信した信号に、マクロビジョン(Macrovision)信号や、CGMS-A(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、VHS方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力I/F140で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

【0333】また、例えば、CGMS-A信号は、デジタル信号のコピー制御に用いられるCGMS信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、1度だけコピーして良いもの(Copy-one-generation)、またはコピーが禁止されているもの(Copy-never)のうちのいずれであることを表す。

【0334】従って、CGMS-A信号が、入出力I/F140で受信した信号に含まれ、かつ、そのCGMS-A信号が、Copy-freelyやCopy-one-generationを表している場合には、アナログコンテンツは、コピー可能であると判定される。また、CGMS-A信号が、Copy-neverを表している場合には、アナログコンテンツは、コピー可能でないと判定される。

【0335】さらに、例えば、マクロビジョン信号も、CGMS-A信号も、入出力I/F4で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

【0336】ステップS4012において、アナログコンテンツがコピー可能でないと判定された場合、ステップS4013乃至S4017をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体10に記録されない。

【0337】また、ステップS4012において、アナログコンテンツがコピー可能であると判定された場合、ステップS4013に進み、以下、ステップS4013乃至S4017において、図3(B)のステップS322乃至S326における処理と同様の処理が行われ、これにより、コンテンツがデジタル変換、MPEG符号化、TS処理、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

【0338】なお、入出力I/F140で受信したアナログ信号に、CGMS-A信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのCGMS-A信号も、記録媒体に記録される。即ち、

図10で示したCCIもしくはその他の情報の部分に、この信号が記録される。この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【0339】[再生処理におけるコピー制御] 次に、記録媒体に記録されたコンテンツを再生して、デジタルコンテンツとして外部に出力する場合においては、図45(A)のフローチャートにしたがった再生処理が行われる。図45(A)の処理について説明する。まず最初に、ステップS4101、S4102、S4103において、図4(A)のステップS401、S402、S403における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段150において復号処理がなされ、TS処理がなされる。各処理が実行されたデジタルコンテンツは、バス110を介して、入出力I/F120に供給される。

【0340】入出力I/F120は、ステップS4104において、そこに供給されるデジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力I/F120に供給されるデジタルコンテンツにEMI、あるいは、EMIと同様にコピー制御状態を表す情報(コピー制御情報)が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【0341】また、例えば、入出力I/F120に供給されるデジタルコンテンツにEMI等のコピー制御情報が含まれる場合、従って、コンテンツの記録時に、DTCの規格にしたがって、EMI等のコピー制御情報が記録された場合には、そのEMI(記録されたEMI(Recorded EMI))等のコピー制御情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。また、EMI等のコピー制御情報が、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないと判定される。

【0342】なお、一般的には、記録されたEMI等のコピー制御情報が、Copy-one-generationやCopy-neverであることはない。Copy-one-generationのEMIは記録時にNo-more-copiesに変換され、また、Copy-neverのEMIを持つデジタルコンテンツは、記録媒体に記録されないからである。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【0343】ステップS4104において、コンテンツが、後でコピー可能なものであると判定された場合、ス

ステップS4105に進み、入出力I/F120は、そのデジタルコンテンツを、外部に出力し、再生処理を終了する。

【0344】また、ステップS4104において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップS4106に進み、入出力I/F120は、例えば、DTC Pの規格等にしがって、デジタルコンテンツを、そのデジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【0345】即ち、例えば、上述のように、記録されたEMI等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【0346】このため、入出力I/F120は、DTC Pの規格にしがたい、相手の装置との間で認証を相互に行い、相手が正当な装置である場合（ここでは、DTC Pの規格に準拠した装置である場合）には、デジタルコンテンツを暗号化して、外部に出力する。

【0347】次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図45(B)のフローチャートにしたがった再生処理が行われる。図45(B)の処理について説明する。ステップS4111乃至S4115において、図4(B)のステップS421乃至S425における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、TS処理、MPEGデコード、D/A変換が実行される。これにより得られるアナログコンテンツは、入出力I/F140で受信される。

【0348】入出力I/F140は、ステップS4116において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、記録されていたコンテンツにEMI等のコピー制御情報がいっしょに記録されていない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【0349】また、コンテンツの記録時に、たとえばDTC Pの規格にしがって、EMI等のコピー制御情報が記録された場合には、その情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

【0350】また、EMI等のコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copies

として扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないと判定される。

【0351】さらに、例えば、入出力I/F140に供給されるアナログコンテンツにCGMS-A信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにCGMS-A信号が記録された場合には、そのCGMS-A信号が、Copy-freelyであるときに

10 は、アナログコンテンツは、後でコピー可能なものであると判定される。また、CGMS-A信号が、Copy-neverであるときには、アナログコンテンツは、後でコピー可能なものでないと判定される。

【0352】ステップS4116において、コンテンツが、後でコピー可能であると判定された場合、ステップS4117に進み、入出力I/F140は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

【0353】また、ステップS4116において、コンテンツが、後でコピー可能でないと判定された場合、ステップS4118に進み、入出力I/F140は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【0354】即ち、例えば、上述のように、記録されたEMI等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【0355】このため、入出力I/F140は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表すCGMS-A信号を付加して、外部に出力する。また、例えば、記録されたCGMS-A信号が、Copy-neverである場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力I/F4は、CGMS-A信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

【0356】以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

【0357】〔データ処理手段の構成〕なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段150は暗号化/復号LSIとして構成することも可能であるが、汎用のコンピュータや、1チップ

のマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。同様にTS処理手段300も処理をソフトウェアによって実行することが可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや1チップのマイクロコンピュータ等にインストールされる。図46は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【0358】プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク4205やROM4203に予め記録しておくことができる。あるいは、プログラムはフロッピー（登録商標）ディスク、CD-ROM (Compact Disc Read Only Memory), MO (Magnetooptical) ディスク, DVD (Digital Versatile Disc), 磁気ディスク、半導体メモリなどのリムーバブル記録媒体4210に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体4210は、いわゆるパッケージソフトウェアとして提供することができる。

【0359】なお、プログラムは、上述したようなリムーバブル記録媒体4210からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部4208で受信し、内蔵するハードディスク4205にインストールすることができる。

【0360】コンピュータは、CPU (Central Processing Unit) 4202を内蔵している。CPU 4202には、バス4201を介して、入出力インタフェース4211が接続されており、CPU 4202は、入出力インタフェース4210を介して、ユーザによって、キーボードやマウス等で構成される入力部4207が操作されることにより指令が入力されると、それにしたがって、ROM (Read Only Memory) 4203に格納されているプログラムを実行する。

【0361】あるいは、CPU 4202は、ハードディスク4205に格納されているプログラム、衛星若しくはネットワークから転送され、通信部4208で受信されてハードディスク4205にインストールされたプログラム、またはドライブ4209に装着されたリムーバブル記録媒体4210から読み出されてハードディスク4205にインストールされたプログラムを、RAM (Random Access Memory) 4204にロードして実行する。

【0362】これにより、CPU 4202は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、C

PU 4202は、その処理結果を、必要に応じて、例えば、入出力インタフェース4211を介して、LCD (Liquid Crystal Display) やスピーカ等で構成される出力部4206から出力、あるいは、通信部4208から送信、さらには、ハードディスク4205に記録させる。

【0363】ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【0364】また、プログラムは、1のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【0365】なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、1チップの暗号化／復号LSIで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図1および図2に示すCPU 170が実行する1つのソフトウェアモジュールとして実現することも可能である。同様に、TS処理手段300の処理もCPU 170が実行する1つのソフトウェアモジュールとして実現することが可能である。

【0366】〔記録媒体の製造装置および方法〕次に、上述した本発明の情報記録媒体を製造する本発明の情報記録媒体製造装置および方法について説明する。

【0367】図47には、記録媒体を製造すると共に、記録媒体に対してディスクID (Disk ID), 有効化キープブロック: EKB (Enabling Key Block) および、暗号化されたマスターキーまたは暗号化されたメディアキーを記録するディスク製造装置の概略構成を示す。

【0368】この図47に示すディスク製造装置は、図示しない組立工程により既に組み立てられている情報記録媒体に対して、ディスクID (Disk ID), 有効化キープブロック: EKB (Enabling Key Block) および、暗号化されたマスターキーまたは暗号化されたメディアキーを記録し、前述の秘密情報を記録する。さらに、必要に応じてマスターキーのプレ (pre-recording) 記録世代情報 (Generation#n) も併せて記録する。

【0369】ディスク製造装置4300は、ディスクID (Disk ID), 有効化キープブロック: EKB (Enabling Key Block) および、暗号化されたマスターキーまたは暗号化されたメディアキーをあらかじめ格納しているメモリ4302もしくはその他の記憶手段と、記録媒体4350に対する読み書きを行う記録媒体I/F 4303と、他の装置とのI/Fとなる入出力I/F 4304と、それらを制御する制御部4301、これらを接続するバス4305を備えている。

【0370】なお、図47の構成では、メモリ4302および記録媒体I/F4304は、当該製造装置に内蔵されている例を挙げているが、メモリ4302および記録媒体I/F4303は外付けのものであってもよい。

【0371】上記のディスクID (Disk ID) ,有効化キーブロック : EKB (Enabling KeyBlock) および、暗号化されたマスターキーまたは暗号化されたメディアキー、スタンパーID等の秘密情報、マスターキーのプレ (pre-recording) 記録世代情報 (Generation#n) は、たとえば図示しない識別子管理部門、鍵発行センター等により発行されるものであり、上記内蔵あるいは外付けのメモリにあらかじめ格納されている。

【0372】上記メモリ4302に格納されているディスクID (Disk ID) ,有効化キーブロック : EKB (Enabling Key Block) 、スタンパーID等の秘密情報および、暗号化されたマスターキーまたは暗号化されたメディアキーは、制御部4301の制御の下、記録媒体I/F4303を介して記録媒体に記録される。なお、必要に応じてマスターキーのプレ (pre-recording) 記録世代情報 (Generation#n) についても記録する。

【0373】なお、スタンパーID等の秘密情報は、前述の「秘密情報の書き込みおよび再生」欄で説明した例例えば図25、図27等の構成を持つ秘密情報生成処理手段に従って生成されたデータであり、各構成に従って、スタンパーID等の秘密情報についてのデータ変換がなされ、その結果として得られる変換データが記録媒体に書き込まれる。

【0374】また、ディスクID (Disk ID) ,有効化キーブロック : EKB (Enabling KeyBlock) および、暗号化されたマスターキーまたは暗号化されたメディアキー、マスターキーのプレ (pre-recording) 記録世代情報 (Generation#n) は、上述したようにメモリ4302にあらかじめ格納されているものを使用するだけでなく、たとえば入出力I/F4304を介して鍵発行センターから送られてきたものを入手することも可能である。

【0375】図48には、本発明の記録媒体製造方法として、上記記録媒体を製造すると共に、記録媒体に対してディスクID (Disk ID) ,有効化キーブロック : EKB (Enabling Key Block) および、暗号化されたマスターキーまたは暗号化されたメディアキー、マスターキーのプレ (pre-recording) 記録世代情報 (Generation#n) を記録する記録媒体製造方法における製造工程の流れを示す。

【0376】図48において、記録媒体製造方法では、まず、ステップS4401の製造工程として、図示しない公知の組立工程によりDVD、CD等各種記録媒体が組み立てられる。

【0377】次に、ステップS4402の製造工程として、図47の記録媒体製造装置により、製造された記録媒体に対して、ディスクID (Disk ID) ,秘密情報とし

てのスタンパーID (Stamper ID) ,有効化キーブロック : EKB (Enabling Key Block) および、暗号化されたマスターキーまたは暗号化されたメディアキーの記録処理を実行する。また、必要に応じてマスターキーのプレ (pre-recording) 記録世代情報 (Generation#n) を記録する。

【0378】以上のディスク製造処理プロセスにより、記録媒体は、ディスクID (Disk ID) ,有効化キーブロック : EKB (Enabling Key Block) および、暗号化されたマスターキーまたは暗号化されたメディアキー、および秘密情報としてのスタンパーIDを記録した状態で製造工場から出荷される。また、必要に応じてマスターキーのプレ (pre-recording) 記録世代情報 (Generation#n) を記録した後、製造工場から出荷される。

【0379】なお、秘密情報として記録するのはスタンパーIDに限らず、ディスク毎に異なって設定されるディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキー等、様々な識別データ、暗号処理鍵をディスクに格納する秘密情報として記録してもよい。記録再生装置においては、これらの様々な秘密情報を適用してコンテンツの暗号処理鍵を生成する。

【0380】[EKBのフォーマット] 図49に有効化キーブロック (EKB : Enabling Key Block) のフォーマット例を示す。バージョン4501は、有効化キーブロック (EKB : Enabling KeyBlock) のバージョンを示す識別子である。デブス4502は、有効化キーブロック (EKB : Enabling Key Block) の配布先のデバイスに対する階層ツリーの階層数を示す。データポイント4503は、有効化キーブロック (EKB : Enabling Key Block) 中のデータ部の位置を示すポイントであり、タグポイント4504はタグ部の位置、署名ポイント4505は署名の位置を示すポイントである。データ部4506は、例えば更新するノードキーを暗号化したデータを格納する。

【0381】タグ部4507は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図50を用いて説明する。図50では、データとして先に図12(A)で説明した有効化キーブロック (EKB) を送付する例を示している。この時のデータは、図50の右の表に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーK(t)Rが含まれているので、トップノードアドレスはKRとなる。

【0382】暗号化キーの最上段のデータEnc(K(t)0, K(t)R)は、図50の左の階層ツリーに示す位置にある。ここで、次のデータは、Enc(K(t)00, K(t)0)であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが

0、ない場合は1が設定される。タグは{左(L)タグ、右(R)タグ}として設定される。最上段のデータ Enc(K(t)0, K(t)R)の左にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、すべてのデータにタグが設定され、図50(c)に示すデータ列、およびタグ列が構成される。

【0383】ツリーのノード処理の順番として、同一段の幅方向を先に処理する幅優先(breadth first)処理と、深さ方向を先に処理する深さ優先(depth first)処理のいずれかを用いるのが好適である。

【0384】図49に戻って、EKBフォーマットについてさらに説明する。署名(Signature)は、有効化キーブロック(EKB)を発行した例えば鍵管理センタ、コンテンツロバイダ、決済機関等が実行する電子署名である。EKBを受領したデバイスは署名検証によって正当な有効化キーブロック(EKB)発行者が発行した有効化キーブロック(EKB)であることを確認する。

【0385】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。例えば、前述したように、実施例においては、ディスクに格納する特定のデータ書き込み処理、再生処理を要求される秘密情報をスタンパーIDとした例を説明したが、スタンパーIDに限らず、ディスク毎に異なって設定されるディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキー等、様々な識別データ、暗号処理鍵をディスクに格納する秘密情報として設定することが可能である。実施例においては、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0386】

【発明の効果】上述したように、本発明の構成においては、記録媒体に、あらかじめその書き込み/読出し方法が解析困難な、特殊の読み出し方法でのみ読み取り可能な秘密情報の信号を格納し、この記録媒体に対する音楽データ、画像データ等のコンテンツの記録あるいは再生を行う際のコンテンツ暗号化あるいは復号処理用暗号鍵に、上記の秘密情報を作用させる構成とした。従って、特定の読み取り方法を実行可能な正当デバイスにおいてのみ、秘密情報の読み取り、コンテンツの暗号処理鍵の生成が可能となり、秘密情報の読み取り方法の実行できないデバイスにおけるコンテンツ再生を効果的に防止することが可能となる。

【0387】また、本発明の構成においては、特殊の読み出し方法でのみ読み取り可能な秘密情報は、正当なデバイス、すなわち秘密情報の読み取り方法を実行可能なデバイスでのみ読み取られ、たとえばLSI内に実装さ

れて高度に保護された暗号鍵の生成を実行する暗号処理部においてセキュアな保護の下にコンテンツ暗号処理用の鍵生成処理に使用される構成であり、秘密情報が外部からの読み取り可能なメモリ上に格納されない。従って、秘密情報の漏洩の可能性がなく、不正なコンテンツの再生処理を効果的に防止することが可能となる。

【0388】また、本発明の構成によれば、ツリー(木)構造の鍵配布構成により、マスターキーやメディアキーの更新データを有効化キーブロック(EKB)とともに送信し、送信したマスターキーやメディアキーと、特殊な読み取り手法でのみ読み取り可能な秘密情報とに基づいてコンテンツ暗号化あるいは復号処理用暗号鍵生成処理を実行する構成としたので、秘密情報についての特殊な読み取り方法を実行可能で、かつツリー構造の鍵配布構成により鍵の配布された正当デバイスでのみコンテンツの利用が可能となる。

【図面の簡単な説明】

【図1】本発明の情報記録再生装置の構成例(その1)を示すブロック図である。

【図2】本発明の情報記録再生装置の構成例(その2)を示すブロック図である。

【図3】本発明の情報記録再生装置のデータ記録処理フローを示す図である。

【図4】本発明の情報記録再生装置のデータ再生処理フローを示す図である。

【図5】本発明の情報記録再生装置において処理されるデータフォーマットを説明する図である。

【図6】本発明の情報記録再生装置におけるトランスポート・ストリーム(TS)処理手段の構成を示すブロック図である。

【図7】本発明の情報記録再生装置において処理されるトランスポート・ストリームの構成を説明する図である。

【図8】本発明の情報記録再生装置におけるトランスポート・ストリーム(TS)処理手段の構成を示すブロック図である。

【図9】本発明の情報記録再生装置におけるトランスポート・ストリーム(TS)処理手段の構成を示すブロック図である。

【図10】本発明の情報記録再生装置において処理されるブロックデータの付加情報としてのブロック・データの構成例を示す図である。

【図11】本発明の情報記録再生装置に対するマスターキー、メディアキー等の鍵の暗号化処理について説明するツリー構成図である。

【図12】本発明の情報記録再生装置に対するマスターキー、メディアキー等の鍵の配布に使用される有効化キーブロック(EKB)の例を示す図である。

【図13】本発明の情報記録再生装置におけるマスターキーの有効化キーブロック(EKB)を使用した配布例

と復号処理例を示す図である。

【図 14】本発明の情報記録再生装置におけるマスターキーの有効化キープブロック (EKB) を使用した復号処理フローを示す図である。

【図 15】本発明の情報記録再生装置におけるコンテンツ記録処理におけるマスターキーの世代比較処理フローを示す図である。

【図 16】本発明の情報記録再生装置において、データ記録処理時の暗号化処理を説明するブロック図 (その 1) である。

【図 17】本発明の情報記録再生装置において、データ記録処理時の暗号化処理を説明するブロック図 (その 2) である。

【図 18】本発明の情報記録再生装置において、データ記録処理を説明するフローチャートである。

【図 19】本発明の情報記録再生装置におけるディスク固有キーの生成例を説明する図である。

【図 20】本発明の情報記録再生装置において処理される伝送 1394 パケットにおける EMI 格納位置 (5C D T C P 規格) を示す図である。

【図 21】本発明の情報記録再生装置におけるコンテンツ記録をデータ解析記録方式 (Cognizant Mode) によって実行するか、データ非解析記録方式 (Non-Cognizant Mode) で実行するかを決定するプロセスを説明するフロー図である。

【図 22】本発明の情報記録再生装置において、データ記録時のタイトル固有キーの生成処理例を示す図である。

【図 23】本発明の情報記録再生装置におけるブロック・キーの生成方法を説明する図である。

【図 24】本発明の情報記録再生装置におけるタイトル固有キーの生成処理フローを示す図である。

【図 25】本発明の情報記録再生装置におけるスタンパー ID 等の秘密情報の記録処理に適用される変調回路を示す図である。

【図 26】図 25 に示すスタンパー ID 等の秘密情報の再生処理に適用される秘密情報復号処理回路を示す図である。

【図 27】本発明の情報記録再生装置におけるスタンパー ID 等の秘密情報の記録構成例を示す図である。

【図 28】図 27 に示すスタンパー ID 等の秘密情報の再生処理に適用される秘密情報復号処理回路を示す図である。

【図 29】本発明の情報記録再生装置におけるデータ解析記録用キーのみを格納した記録再生装置構成例を示す図である。

【図 30】本発明の情報記録再生装置におけるデータ非解析記録用キーのみを格納した記録再生装置構成例を示す図である。

【図 31】本発明の情報記録再生装置において、データ

再生処理時のコンテンツデータ復号処理を説明するブロック図である。

【図 32】本発明の情報記録再生装置において、データ再生処理を説明するフローチャートである。

【図 33】本発明の情報記録再生装置において、データ再生処理における再生可能制判定処理の詳細を示すフローチャートである。

【図 34】本発明の情報記録再生装置において、データ再生時のタイトル固有キーの生成処理フローを示す図である。

【図 35】本発明の情報記録再生装置におけるメディアキーの有効化キープブロック (EKB) を使用した配布例と復号処理例を示す図である。

【図 36】本発明の情報記録再生装置におけるメディアキーの有効化キープブロック (EKB) を使用した復号処理フローを示す図である。

【図 37】本発明の情報記録再生装置におけるメディアキーを使用したコンテンツ記録処理フローを示す図である。

【図 38】本発明の情報記録再生装置において、メディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図 (その 1) である。

【図 39】本発明の情報記録再生装置において、メディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図 (その 2) である。

【図 40】本発明の情報記録再生装置において、メディアキーを使用したデータ記録処理を説明するフローチャートである。

【図 41】本発明の情報記録再生装置において、メディアキーを使用したデータ再生処理時の暗号化処理を説明するブロック図である。

【図 42】本発明の情報記録再生装置において、メディアキーを使用したデータ再生処理を説明するフローチャートである。

【図 43】本発明の情報記録再生装置において、メディアキーを使用したデータ再生処理における再生可能性判定処理の詳細を示すフローチャートである。

【図 44】本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

【図 45】本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

【図 46】本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

【図 47】本発明の情報記録再生装置において使用される情報記録媒体を製造する製造装置の構成を示すブロック図である。

【図 48】本発明の情報記録再生装置において使用され

る情報記録媒体を製造する製造処理の処理フローを示す図である。

【図49】本発明の情報記録再生装置において使用される有効化キープブロック (EKB) のフォーマット例を示す図である。

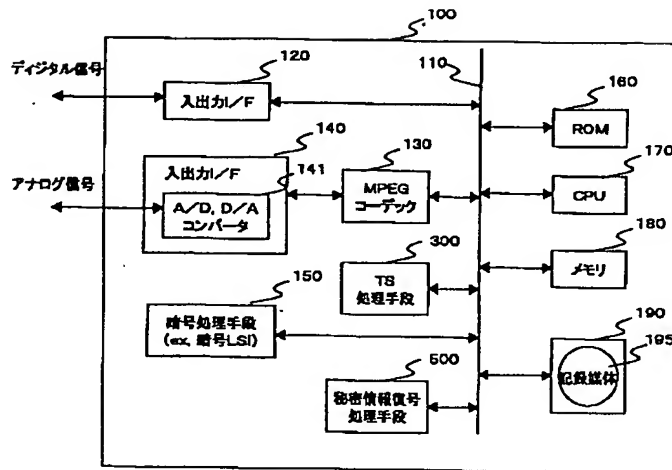
【図50】本発明の情報記録再生装置において使用される有効化キープブロック (EKB) のタグの構成を説明する図である。

【符号の説明】

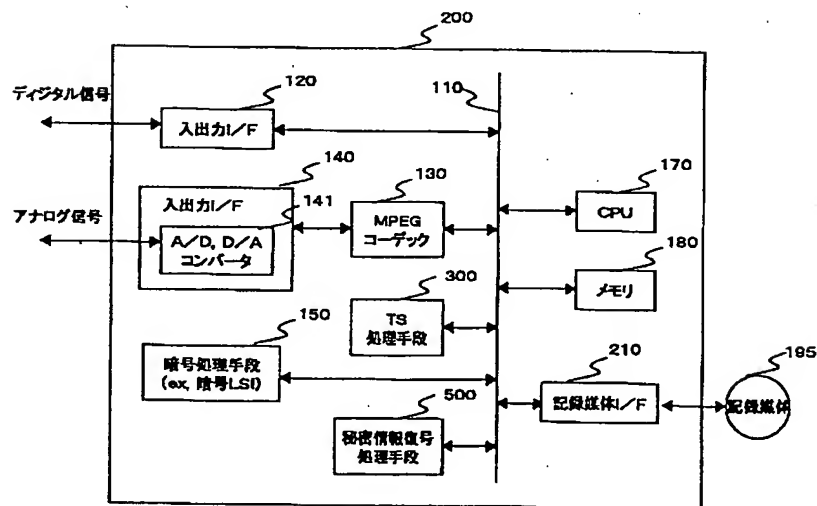
100, 200 記録再生装置
 110 バス
 120 入出力 I/F
 130 MPEGコーデック
 140 入出力 I/F
 141 A/D, D/Aコンバータ
 150 暗号処理手段
 160 ROM
 170 CPU
 180 メモリ
 190 ドライブ
 195 記録媒体
 210 記録媒体 I/F
 300 TS処理手段
 500 秘密情報復号処理手段
 600, 607 端子
 602 ビットストリームパーサ
 603 PLL
 604 タイムスタンプ発生回路
 605 ブロックシード付加回路
 606 スムージングバッファ
 800, 806 端子
 801 ブロックシード分離回路
 802 出力制御回路
 803 比較器
 804 タイミング発生回路
 805 27MHzクロック
 901, 904, 913 端子
 902 MPEGビデオエンコーダ
 903 ビデオストリームバッファ
 905 MPEGオーディオエンコーダ
 906 オーディオストリームバッファ
 908 多重化スケジューラ
 909 トランスポートパケット符号化器
 910 到着タイムスタンプ計算手段
 911 ブロックシード付加回路
 912 スムージングバッファ

976 スイッチ
 1041 PLL回路
 1042 タイミングジェネレータ
 1043 同期パターン発生回路
 1045 M系列発生回路
 1046 演算回路
 1047 乱数発生回路
 1048 データセクタ
 1049 データセクタ
 1081 PLL回路
 1082 同期検出回路
 1083 M系列発生回路
 1084 乗算回路
 1085 積分回路
 1086 判定回路
 1160 PLL回路
 1161 同期検出回路
 1162 タイミングジェネレータ
 1163 フリップフロップ
 1164 最大値検出回路
 1165 パラレルシリアル変換回路
 4202 CPU
 4203 ROM
 4204 RAM
 4205 ハードディスク
 4206 出力部
 4207 入力部
 4208 通信部
 4209 ドライブ
 4210 リムーバブル記録媒体
 4211 入出力インタフェース
 4300 ディスク製造装置
 4301 制御部
 4302 メモリ
 4303 記録媒体 I/F
 4304 入出力 I/F
 4305 バス
 4350 記録媒体
 4501 バージョン
 4502 デプス
 4503 データポインタ
 4504 タグポインタ
 4505 署名ポインタ
 4506 データ部
 4507 タグ部
 4508 署名

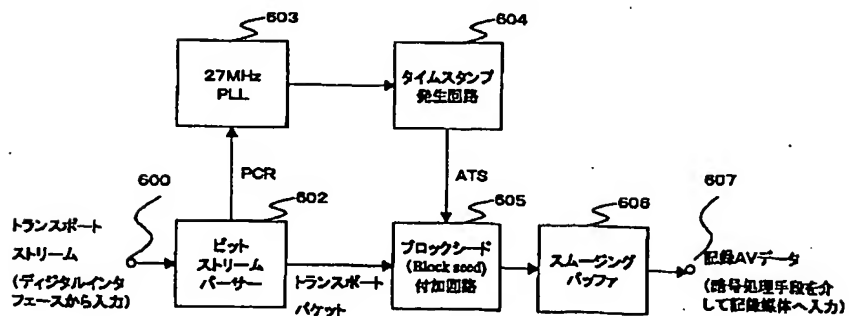
【図1】



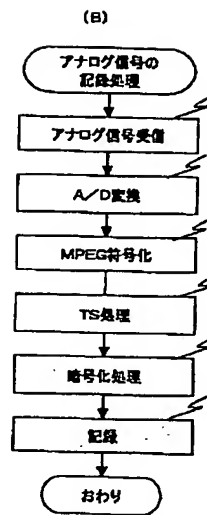
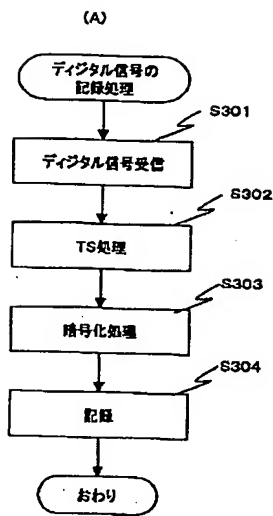
【図2】



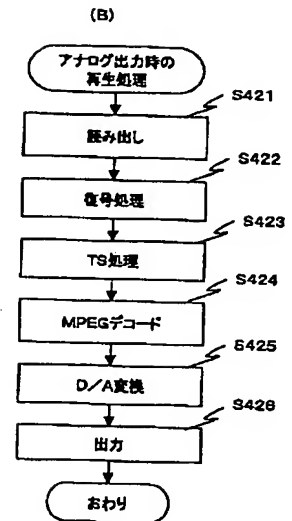
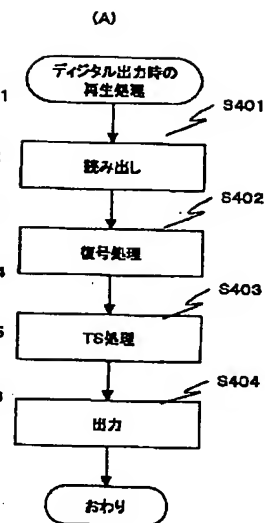
【図6】



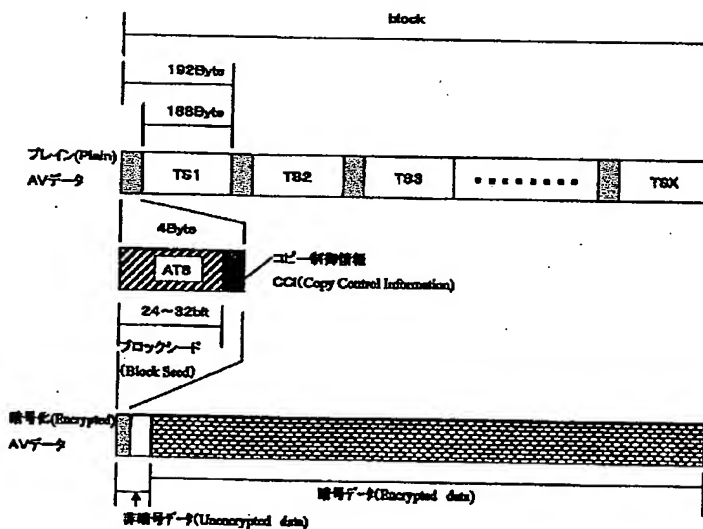
【図3】



【図4】



【図5】



(A) キー更新ブロック(KRB: Key Renewal Block) 例1

デバイス0, 1, 2にt時点でのルートキー-K(t)Rを送付

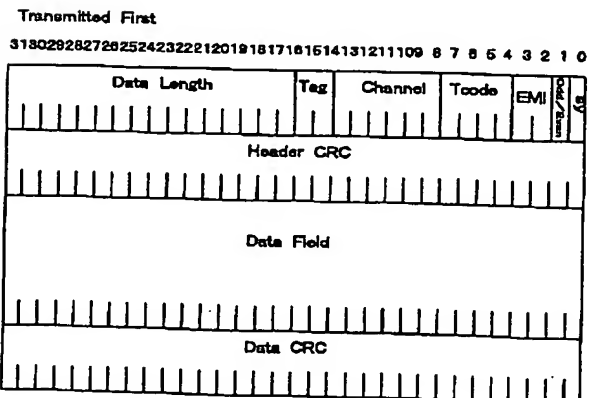
世代(Generation): t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) キー更新ブロック(KRB: Key Renewal Block) 例2

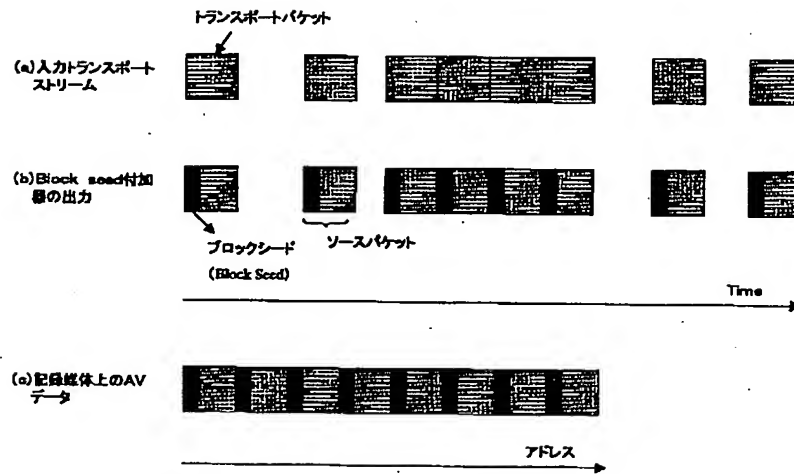
デバイス0, 1, 2にt時点でのルートキー-K(t)Rを送付

世代(Generation): t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

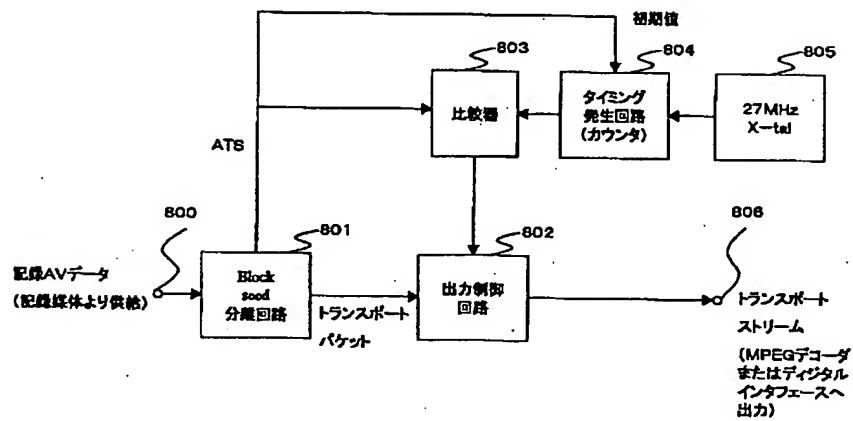
【図20】



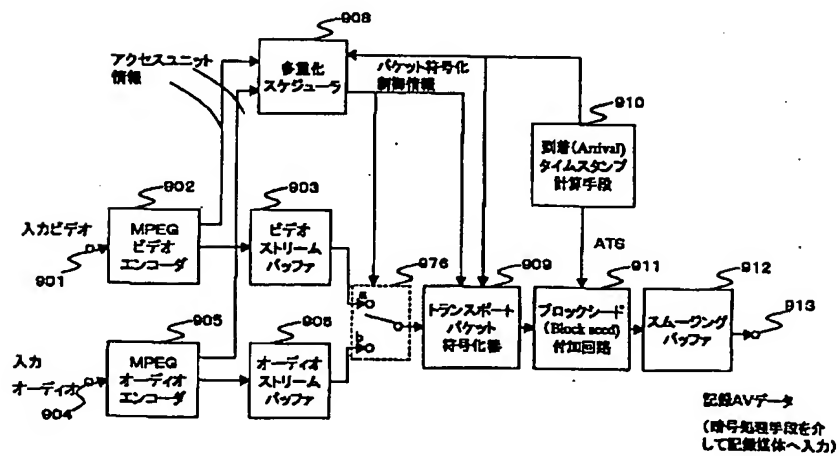
【図7】



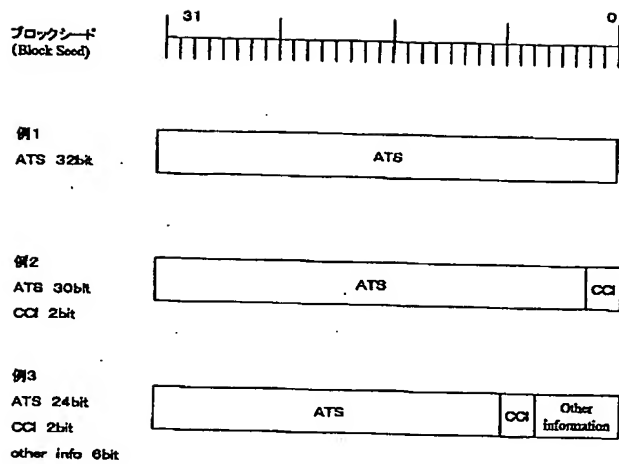
【図8】



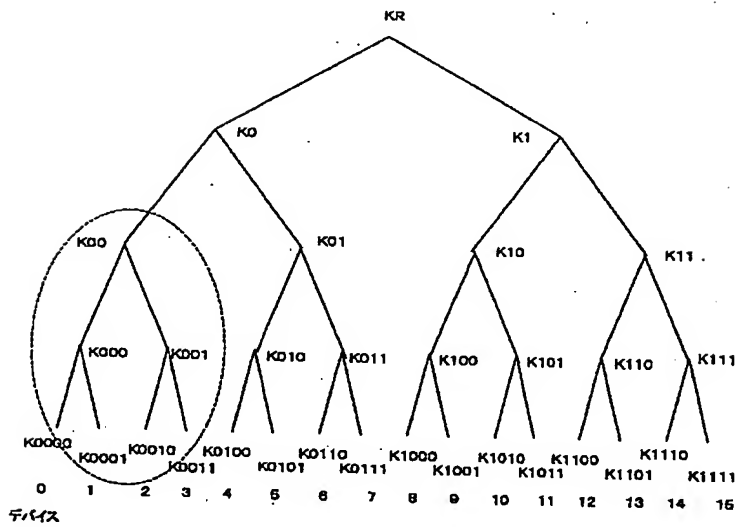
【図9】



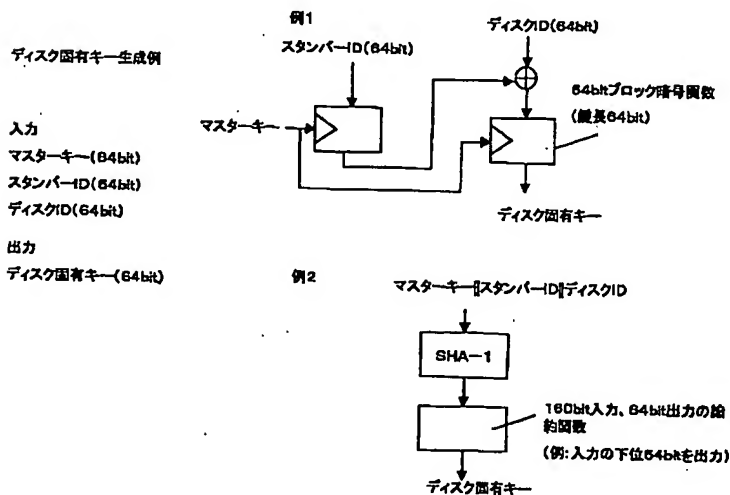
【図10】



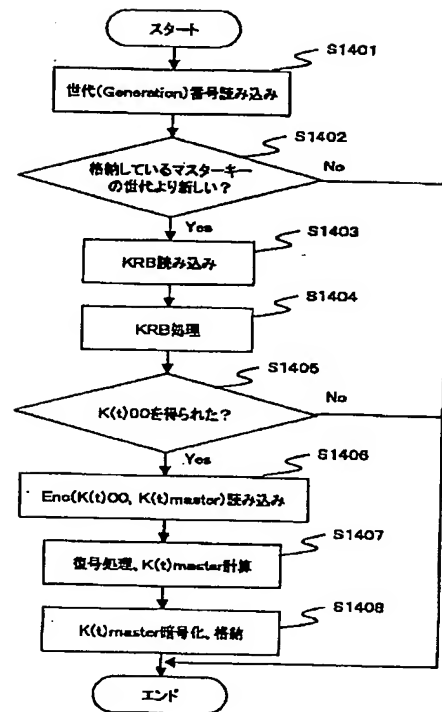
【図11】



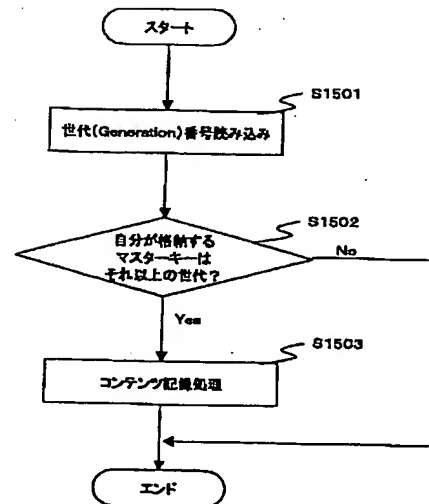
【図19】



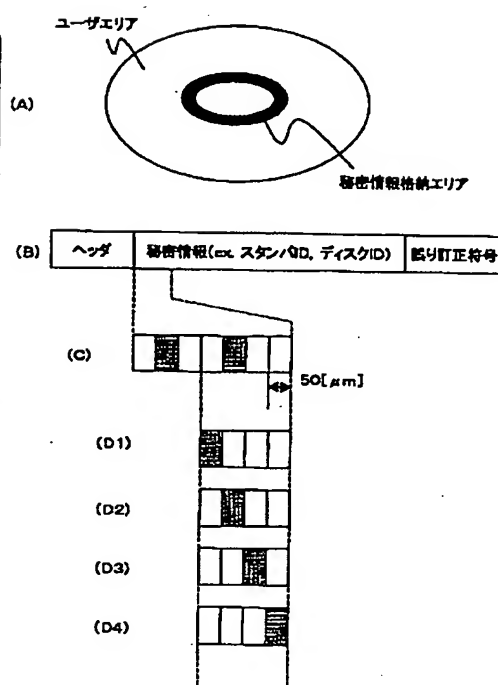
【図14】



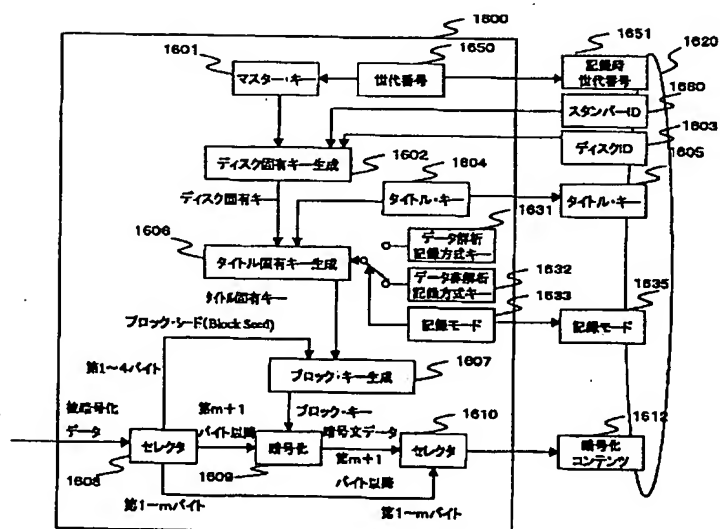
【図15】



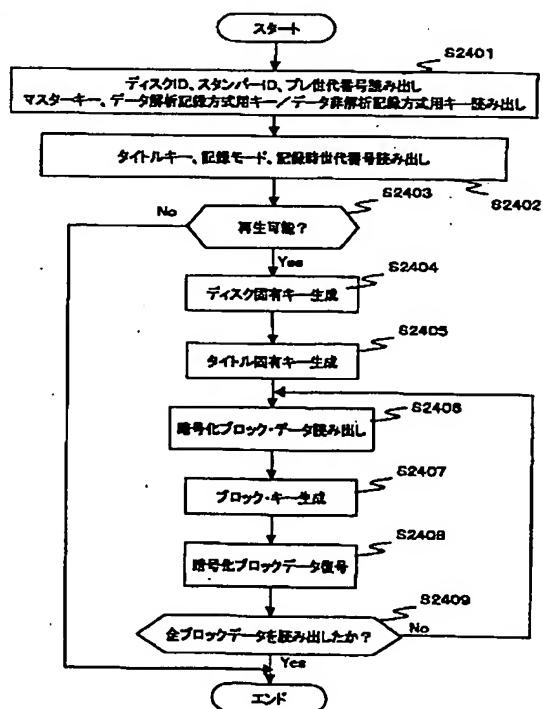
【圖 27】



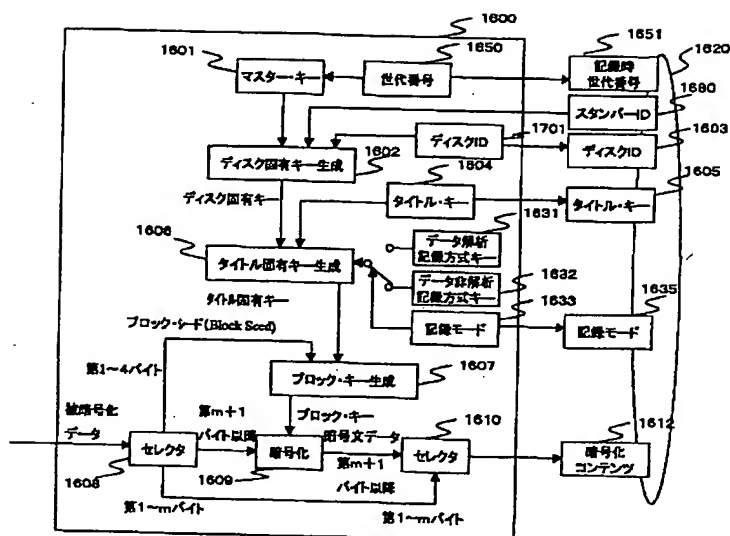
【図 16】



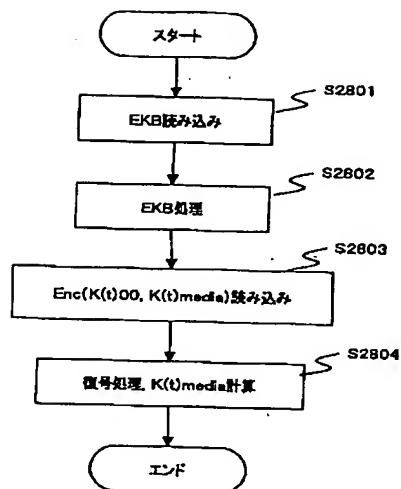
【図 3 2】



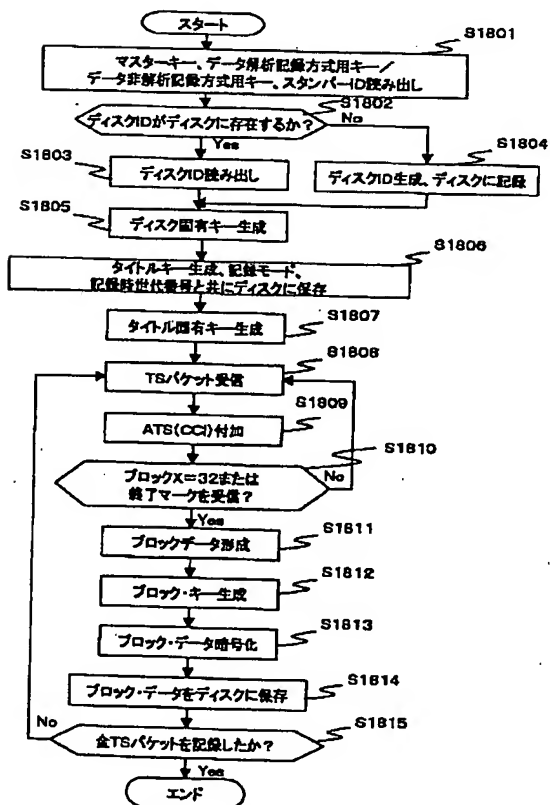
【図17】



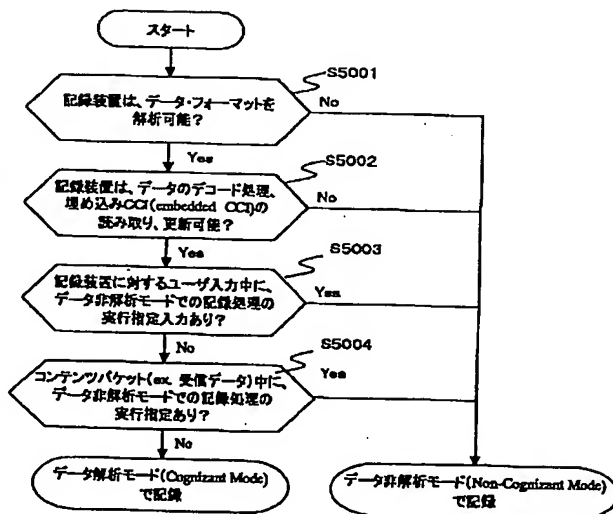
【図36】



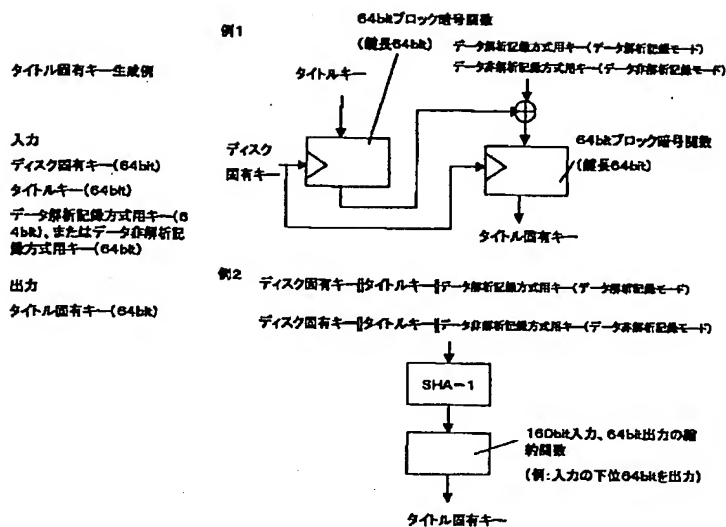
【図18】



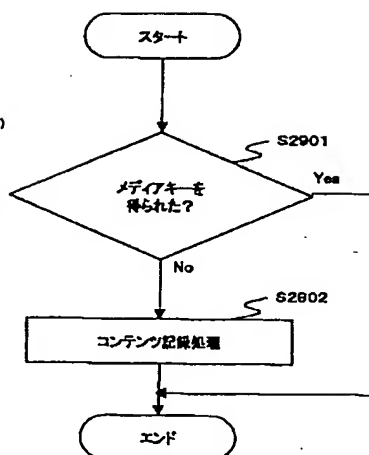
【図21】



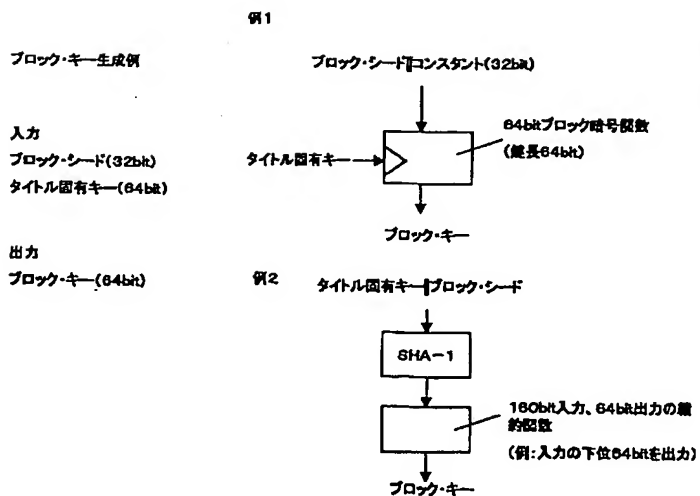
【図22】



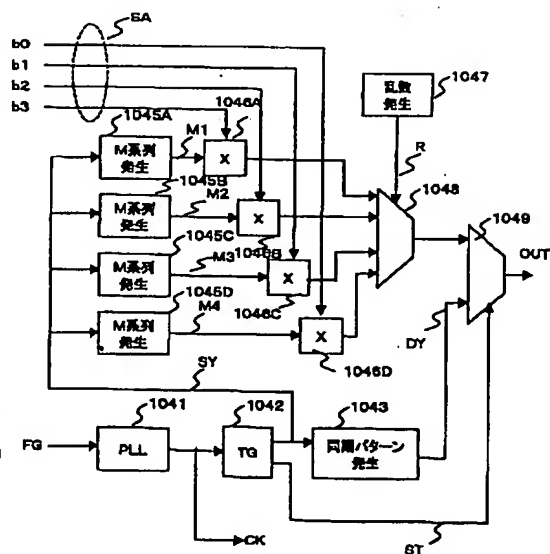
【図37】



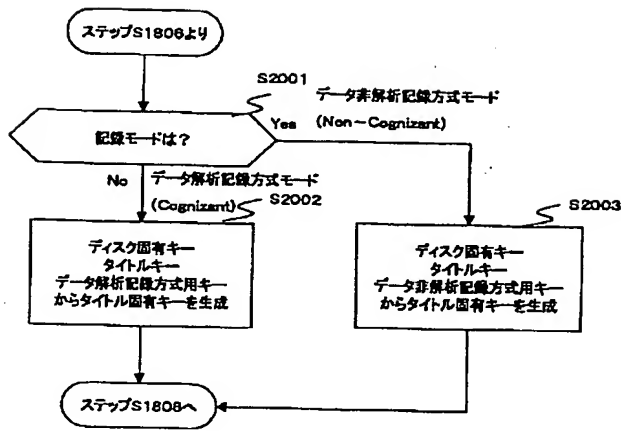
【図23】



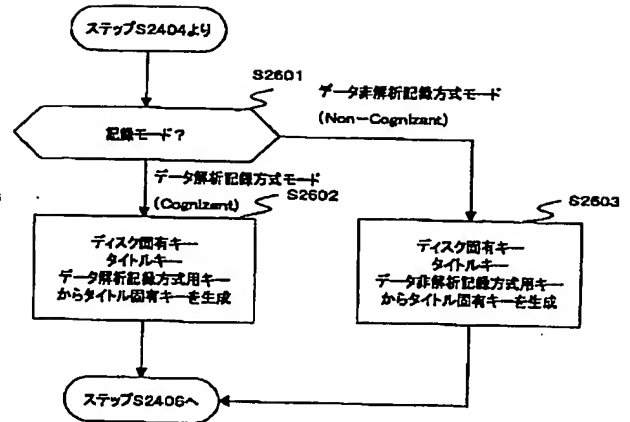
【図25】



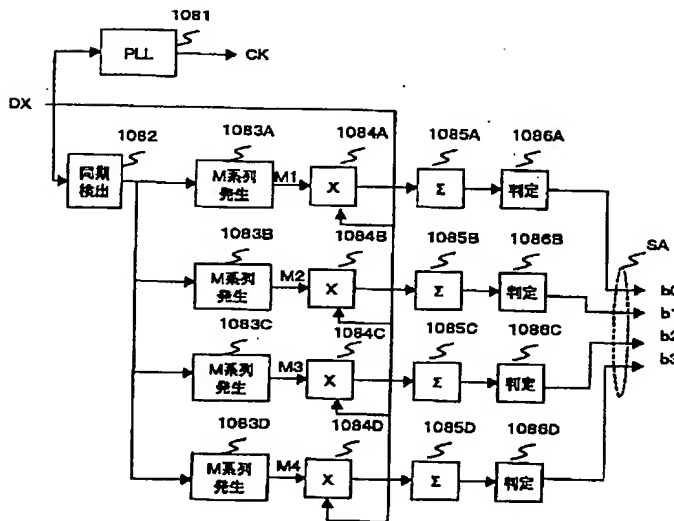
【図24】



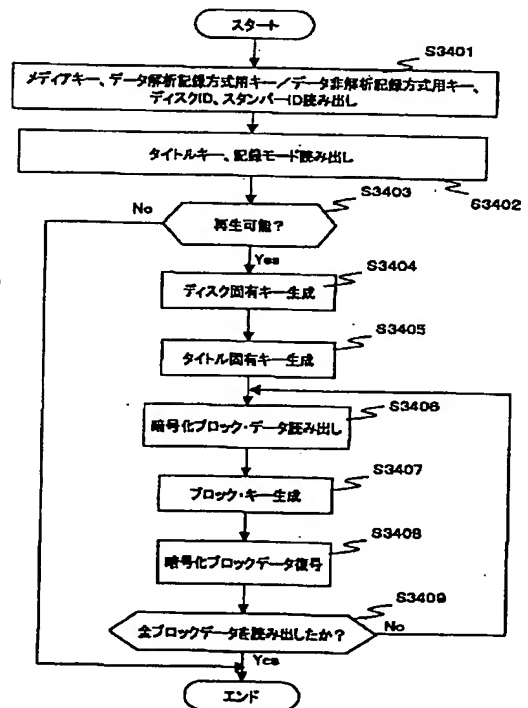
【図34】



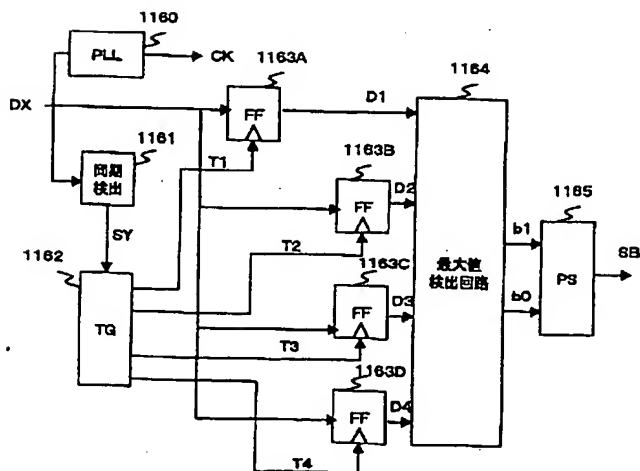
【図26】



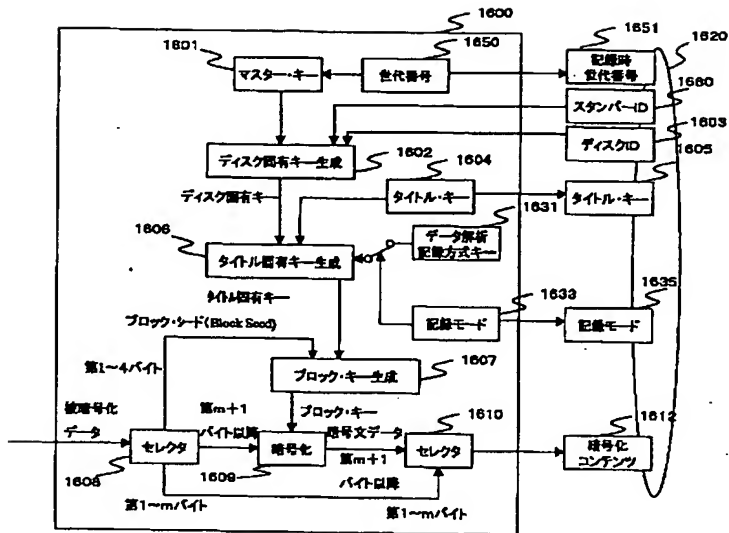
【図42】



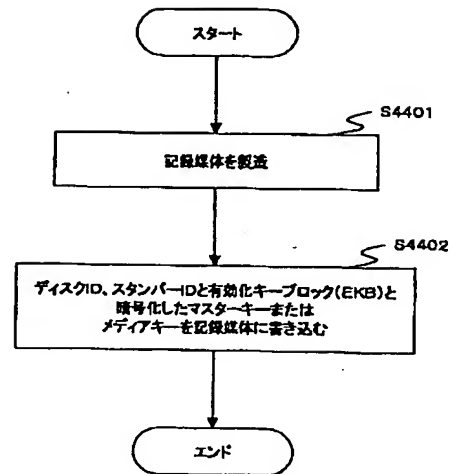
【図28】



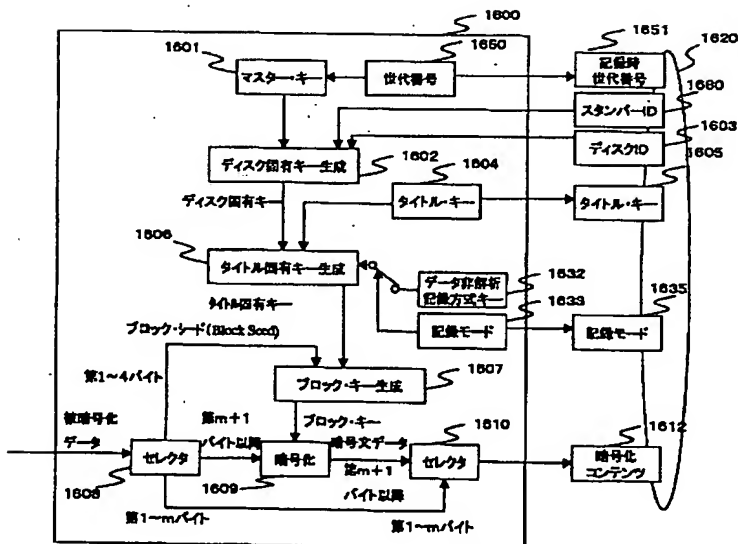
【図29】



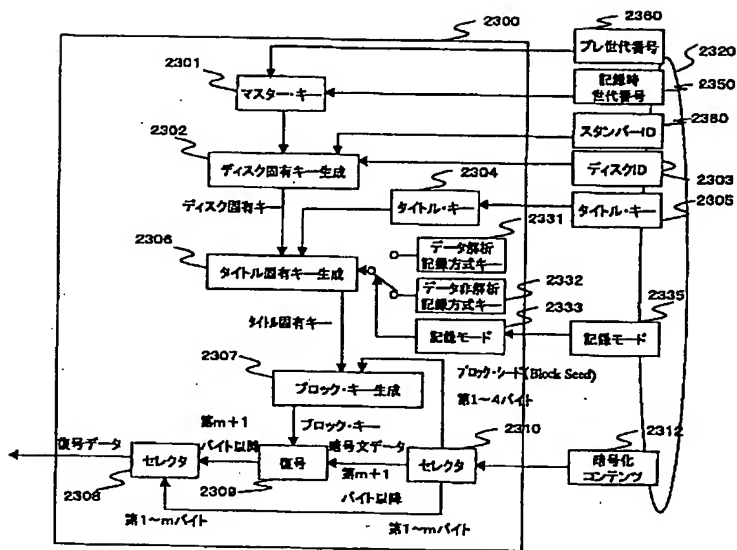
【図48】



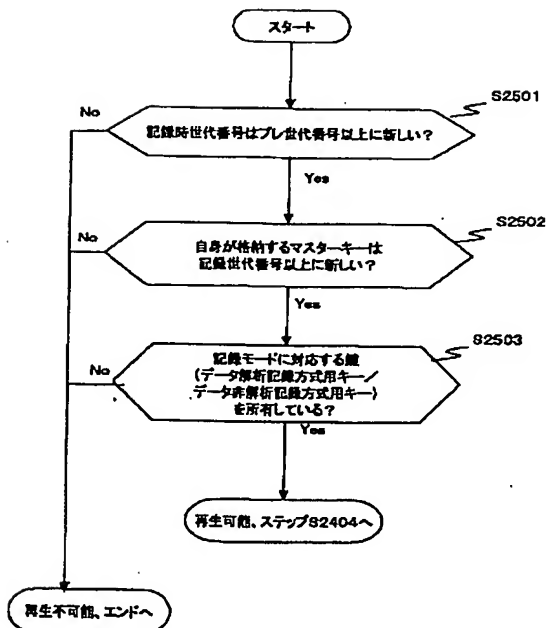
【図30】



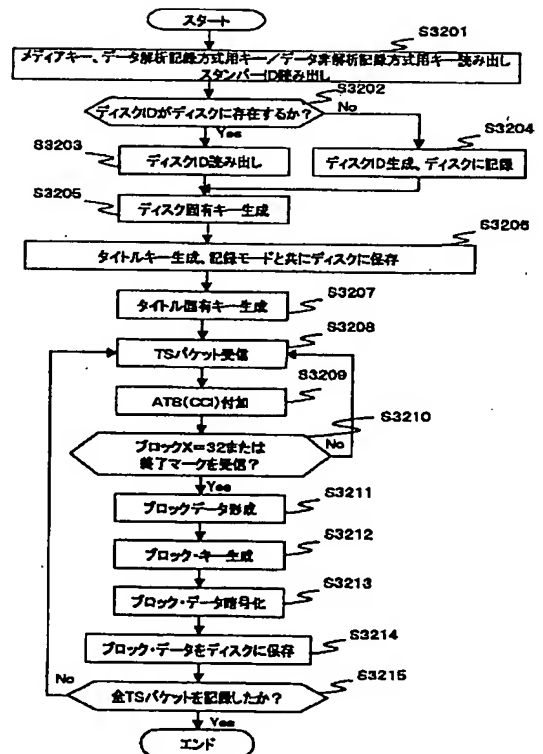
【図31】



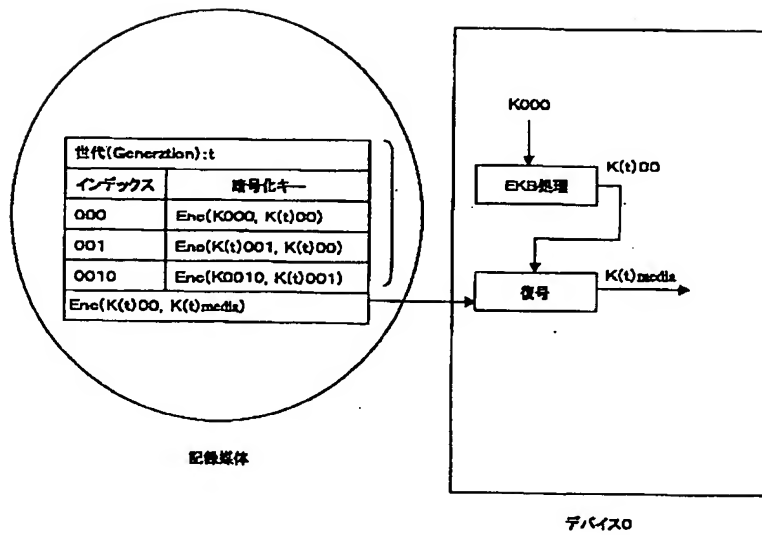
【図33】



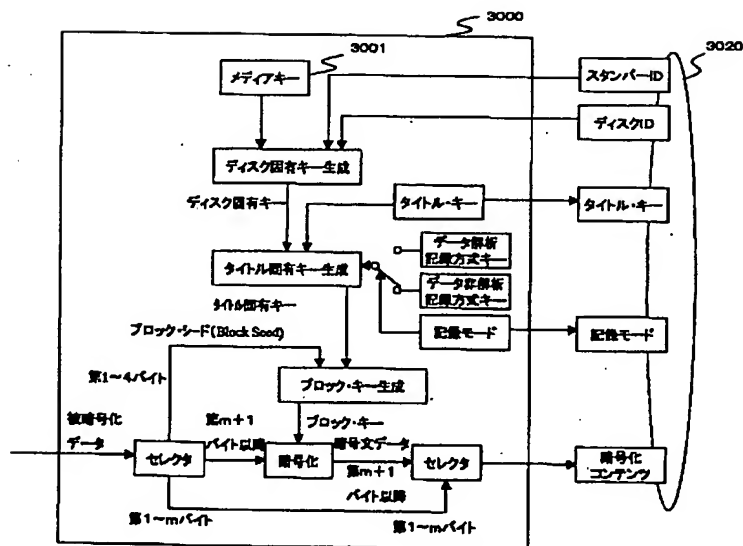
【図40】



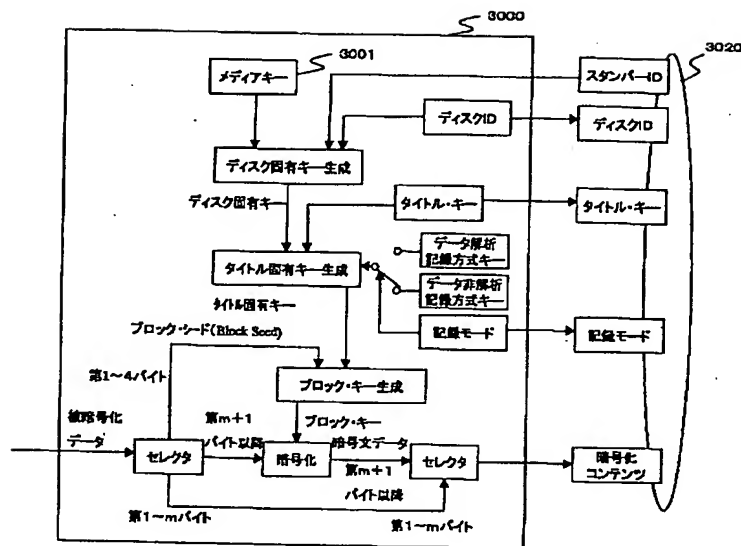
【図35】



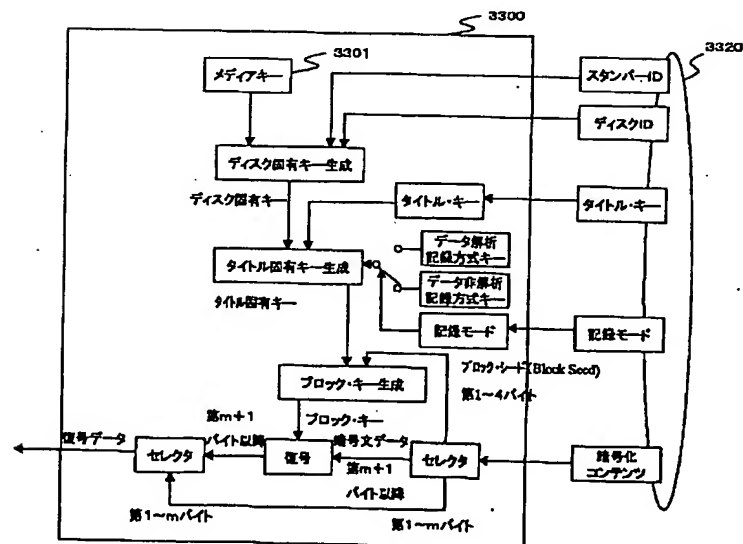
【図38】



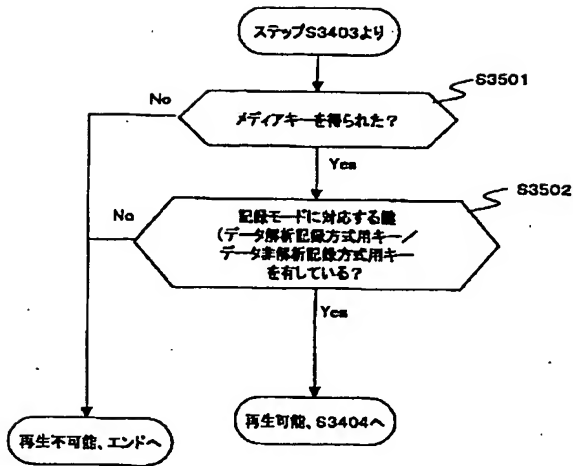
【図39】



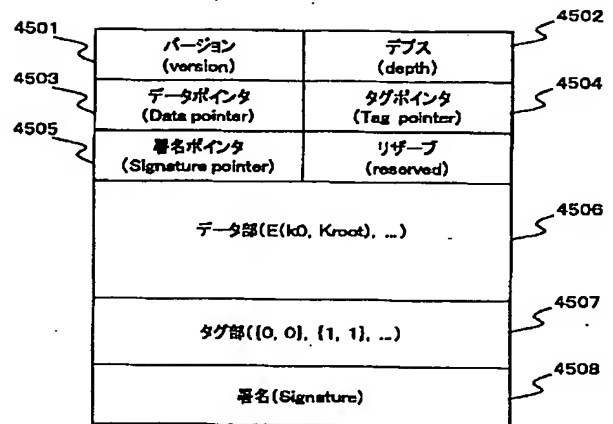
【図41】



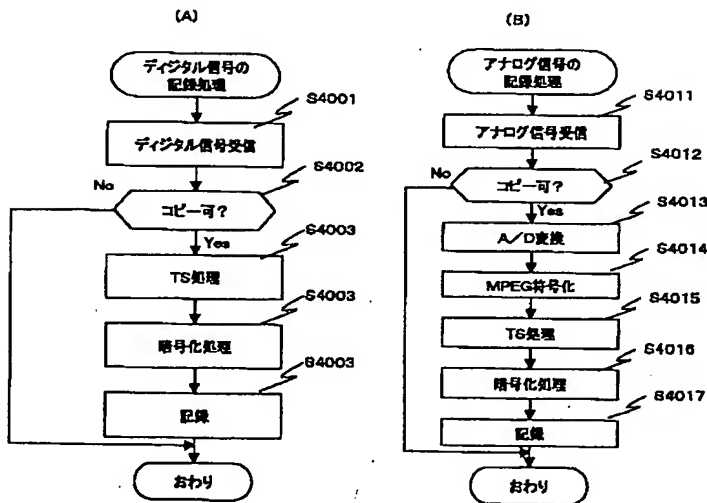
【図43】



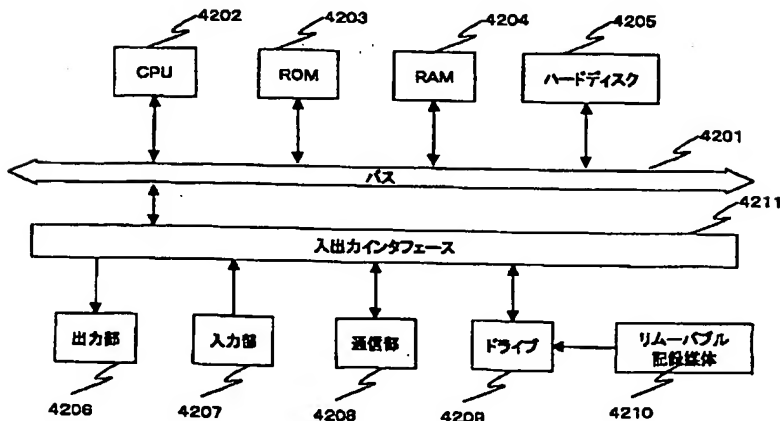
【図49】



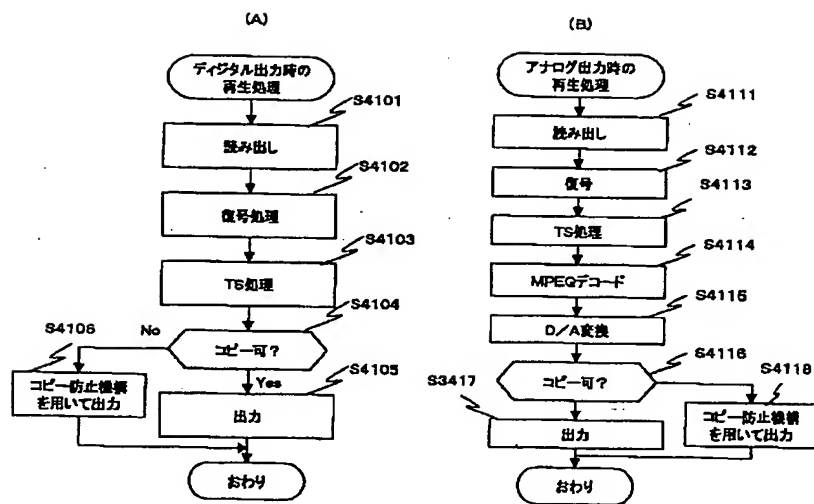
【図44】



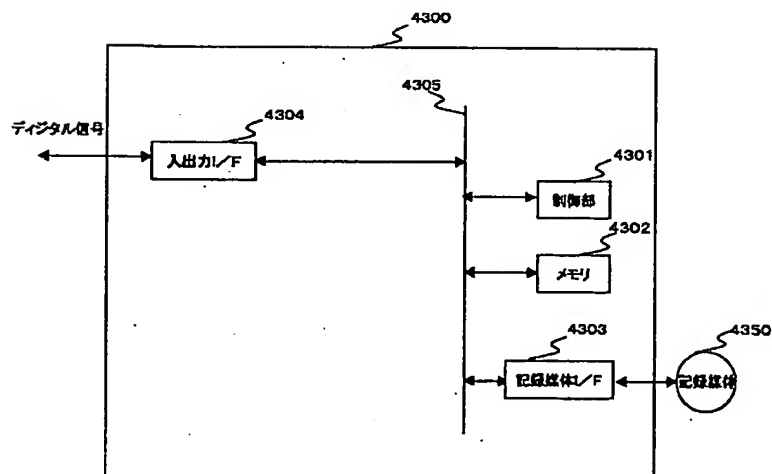
【図46】



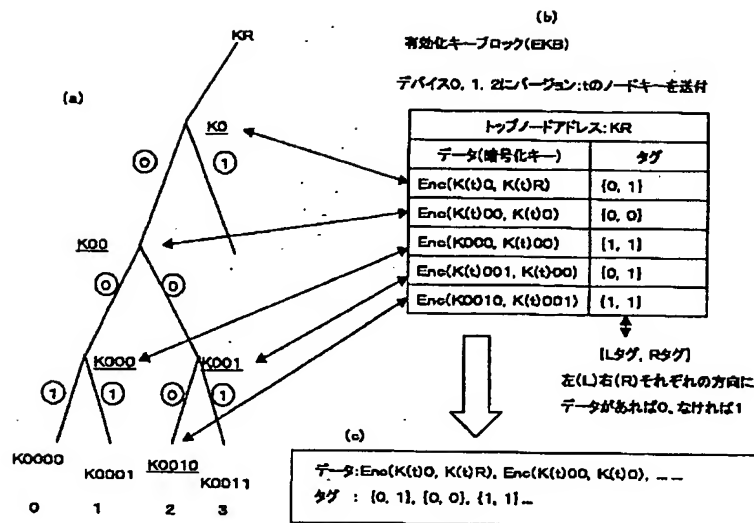
【図45】



【図47】



【図50】



フロントページの続き

Fターム(参考) 5D044 AB01 AB05 AB07 BC02 CC04
 EF05 FG18 GK17 HH13 HH15
 HL06
 5J104 AA01 AA12 AA16 EA04 EA26
 JA03 MA08 NA02 NA31 NA32
 PA14